Gamified Cybersecurity Learning in Capture-the-Flag competitions through the Lens of the Information Search Process

Abstract

Capture the Flag challenges are a popular form of cybersecurity education, where students solve hands-on tasks in a game-like setting. These exercises provide learning experiences with various specific technologies and subjects, as well as a broader understanding of cybersecurity topics. Competitions reinforce and teach problem-solving skills that are applicable in various technical and non-technical environments outside of the competitions. The Information Search Process (ISP) is a framework developed to understand the process by which an individual goes about studying a topic identifying emotional ties connected to each step an individual take. As the individual goes through the problem-solving process, there is a clear flow from uncertainty to clarity, the individual's feelings, thoughts, and actions are all interconnected. This study proposes that as we explore the learning of cybersecurity concepts through the lens of the Information Search Process, within the contexts of Capture-the-Flag competitions, we expect results both along the predicted outcomes, as well as various unknown outcomes. Our overarching hope in performing this research is for three general outcomes. First, an increased understanding of the emotional and intellectual experience of solving a problem, as illustrated by the Information Search Process approach. Second, an increased understanding of how the delivery of a Capture-the-Flag problem affects the learning experience of the participant. Finally, a greater understanding of effective cybersecurity education, in which actionable steps are identified to better teach technical skills and approaches.

Keywords: Cybersecurity, Capture-the-Flag, Information Search Process, affect

Introduction

The Information Search Process (ISP), developed by Carol Kuhlthau (1993), is a framework to understand the process by which a researcher goes about studying a topic. Her paper identifies emotional ties connected to each step a researcher takes. As the researcher goes about studying their topic or argument, there is a clear flow from uncertainty to clarity. Kuhlthau (1993) further explains that in studying a topic, the learner's feelings, thoughts, and actions are all interconnected.

One of the main problems which researchers face in the search for information is that of uncertainty or doubt. Kuhlthau (1993) addresses the different types of uncertainty that a researcher can feel and explains that the transition from uncertainty to certainty is the most pivotal part of the search process.

By identifying their position in the progression of the Information Search Process model, a researcher can more appropriately decide the best course of action to combat the negative emotions they encounter in their learning experience. In doing so, they become more able to experience joy and accomplishment while they gain knowledge.

After its conceptualization in the late 80s and early 90s, Kuhlthau and her associates at Rutgers University revisited their work on the ISP in 2008. With the advancements in technology that had occurred over this span of time, it was necessary to determine whether the ISP model was still effective for evaluating learning in today's digital environment. A study that revisited

the findings of ISP found that the ISP as a "model continues to be a useful theoretical and explanatory framework for user studies in librarianship and information science" (Kuhlthau et al., 2008).

Researchers found it necessary to evaluate the effectiveness of the ISP in describing education in an increasingly digital environment. Kuhlthau discovered that researchers believed that with such readily accessible information at their fingertips, the process would be easier. Resulting information has shown that the ISP is still applicable in a digital age, and that the search for information remains difficult despite increasing access to information on the Internet (Holladay & Li, 2004).

After having revisited the ISP, it is found that the model continued to be useful. The progression of emotions and cognitive responses were still connected to the learning process, and the ISP was still a valuable tool to guide researchers in their search for information.

In 1999, the National Security Agency (NSA) launched the Center of Academic Excellence in Information Assurance Education (CAE-IAE) program. Under this program, an institution could receive the CAE-IAE designation if it passed rigorous curriculum and program requirements.

The NSA's National Cryptologic School manages National Centers of Academic Excellence in Cybersecurity (NCAE-C) program. Federal partners include the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST)/National Initiative on Cybersecurity Education (NICE), the National Science Foundation (NSF), the Department of Defense Office of the Chief Information Officer (DoD-CIO), and U.S. Cyber Command (USCYBERCOM). Currently, the NCAE-C program has over 300 institutions all over the nation with designations in Cyber Defense (CAE-CD), Cyber Research (CAE-R), and Cyber Operations (CAE-CO) (NSA, 2021; CAECC, 2021).

In cybersecurity, there are endless resources available dedicated to helping people learn and develop relevant skills. One area in this vast ecosystem is that of cybersecurity Capture-the-Flag (CtF) competitions. These competitions involve various technical cybersecurity challenges that participants have a limited time to solve. These challenges come in the form of a problem presented with a prompt and are solved by submitting a unique text phrase found at the completion of the problem. These challenges can fall under a wide variety of topics including web vulnerabilities, cryptography, reverse engineering, and more. After the competition finishes, participants often submit written reports of their solutions to the challenges.

Capture-the-Flag competitions have been used as an educational exercise in the field of cybersecurity since 1996. These exercises provide learning experiences with various specific technologies and subjects, as well as a broader understanding of cybersecurity topics (Švábenský *et al*. 2021). Competitions reinforce and teach problem-solving skills that are applicable in various technical and non-technical environments outside of the competitions. The learning process used to solve these challenges is driven by the various gamified aspects that increase interest and participation. Previous research has found that this methodology is effective in teaching such technical skills and topics to students (McDaniel et al. 2016; Leune & Petrilli, 2017). There exists, however, room to more fully understand the emotions and processes that a student encounters throughout the competition. We believe the application of the ISP as revisited and set forth by Kuhlthau is optimal for addressing this topic.

Hypothesis: The Information Search Process provides a relevant framework for evaluating the effectiveness of CTFs in cybersecurity education because of its attention on cognitive and emotional experiences throughout the learning process.

By using the ISP model to evaluate students' emotions during CtF challenges, we hope for a better understanding of the following items: the validity of the Information Search Process in evaluating Capture-the-Flag challenges; the effectiveness of Capture-the-Flag challenges in cybersecurity education; and the areas of improvement for Capture-the-Flag challenges, as identified through the lens of the Information Search Process.

Literature Review

In our study of how the ISP can be applied to cybersecurity education via CtF activities, we read and categorized articles by the themes of the research questions in each of the articles. Our research led us to find commonalities in education, gamification, and Capture-the-Flags in general. We aim to create an effective study examining the relationship between the Information Search Process and Capture-the-Flag competitions.

While the CtF activities are a competitive and effective way to show one's technical abilities, these activities can also help the participants learn and apply new skills in cybersecurity. Research shows that competitions and challenges that force students to work together and apply knowledge resulted in improvement of the students' technical skills, level of interest in the subject, and ability to teach their newfound skills (Cheung, *et al*., 2011). This is a promising result because a student being able to teach a subject that they have been learning is an effective indicator of advanced comprehension.

Subhash and Cudney (2018, p. 192) concluded that found "encouraging support for gamified learning in higher education used in the form of gamification and game-based learning." They further stated that the findings allow higher education universities to employ and explore efficient gamified learning and teaching systems to improve student engagement, motivation, and performance. The successful implementation of gamification and game-based learning give reason to be enthusiastic about their application in higher education.

Capture-the-Flags are typically team events wherein student competitors are forced to apply their previous knowledge in the field in new ways, making them a qualified component of Challenge-Based Learning, meaning that these activities can be shown to increase technical skills and levels of interest in the subject. Another research studied curricula designed with Student Centered Learning ideals, which are methods of education where students are actively involved in deciding the curriculum and have a high degree of choice. Resulting in the idea that such curricula are beneficial to students' information gathering experience because it raises their motivation and satisfaction with their education (O'Neill & McMahon, 2005). Academic game-like competitions such as CtF provide that "high degree of choice" for students, meaning that they are likely to result in increased motivation and satisfaction throughout the learning process.

Within the realm of improving our understanding of students' cognitive experience in education, we find a lot of valuable information in Kuhlthau's ISP. The ISP is a six-stage model of one's *holistic* experience in the process of information seeking. Its added value comes from its acknowledgement of the affective (feelings), cognitive (thoughts), and physical (actions) realms in the process of learning new information. One important finding from Kuhlthau's research was that "the primary objective of information seeking is to accomplish the task that initiated the search, not merely the collection of information as an end in itself" (Kuhlthau, 1993). We believe Capture-the-Flag competitions provide additional intrinsic motivation that would give further reasons for students to invest seriously in their practical education. When Kuhlthau revisited her research years later, she showed that the more a student struggles with the learning process, the deeper their knowledge becomes and the more their confidence grows. It was also shown that higher engagement with material correlates with more positive emotions at the end of the process (Kuhlthau et al., 2008). All the findings in these studies seem to indicate that if there is a way to

increase the students' motivation to learn the content, along with critical thought processes and applications of knowledge, that education would be more beneficial for students.

As CtF competitions are a gamified method of demonstrating cybersecurity skills, we found a survey of literature on gamification to be beneficial. Researcher found that gamification makes learning more fun and engaging without undermining its instructional credibility (Muntean, 2011). Additionally, Subhash and Cudney (2018) found that learning with the help of games elicits positive emotions, making the players feel focused, engaged, accomplished, productive, and motivated. In addition to this, games were shown to improve knowledge acquisition, content mastery, learner motivation, and academic effort. It is clear through these findings that including gamified elements in the learning process will bring numerous positive emotional results.

Finally, we further narrowed our literature survey by examining the findings related to CtF. Capture-the-Flags, which provide typically a more offensive-oriented education, were found to result in a statistically significant higher understanding of network vulnerabilities in an ANOVA test compared to participants of a defensive-only course (Mink & Greifeneder, 2010). Consistent with our findings in the general gamification category, we found that these cybersecurity challenges result in motivation for learning, enjoyment in learning, satisfaction in achieving, and improved practical knowledge (Chothia & Novakovic, 2015). It was also found that CtF provide students with increased confidence in their abilities (Leune & Petrilli, 2017). This occurred because of the practical application that was made possible in these hands-on challenges. It was also found that student motivation is a key predictor of educational outcomes. Additionally, another study showed that participants who attempt a variety of challenges to find those in which they are interested tend to learn more effectively (McDaniel et al., 2016).

In conclusion, CtF provide a concrete application of learned knowledge and a clear direction for future study, which are key components of effective learning. In addition to this, the gamified environment that they create can be shown to be effective at increasing student interaction with the material and overall motivation and satisfaction with the learning process.

Methodology

This study intends to demonstrate that due to the manner that the ISP model weighs emotional experience during information gathering, it is a useful framework to use in evaluating the effectiveness of using CtF competitions in cybersecurity education. Ultimately, we will need both quantitative and qualitative analysis to demonstrate a parallel between the emotions felt when gathering information as described in ISP, and the affective experience of learning cybersecurity skills in CtF competitions. The data used in this paper will come from an observational study conducted by the Brigham Young University Cybersecurity Research Lab in association with the Cybersecurity Student Association of BYU and their end of semester Capture-the-Flag event.

To support our hypothesis, we will need to collect data of cybersecurity students' emotions over the course of a singular CtF competition. In addition to that, we will also perform a longitudinal survey of attitudes towards the field of cybersecurity in general as experience in the field progresses. We believe the following methodology to be a suitable approach for the evaluation of feelings during multifaceted thought processes, as this type of analysis of survey results is very common in papers with comparably-designed hypotheses.

We intend to measure uncertainty, optimism, confusion, frustration, doubt, sense of direction, clarity, confidence, satisfaction, disappointment, and accomplishment using a survey with a 7-point Likert scale. These are the emotions identified in ISP. After completion of a challenge in our CtF, the survey will be offered for a small number of points that sends the

student to a Google Forms page containing the survey. This method should provide sufficiently-unbiased sampling due to the low cost-to-reward ratio of obtaining these points, while still resulting in sufficient motivation for the student to respond to the survey following the completion of each challenge.

The questions take the form of "rate your agreement with the following statements," followed by feeling-centric phrases like "I felt a high degree of confidence in my knowledge and abilities before starting the challenge". The answers on the Likert scale will range from 1, "very strongly disagree", to 7, "very strongly agree", with 4 representing neutral sentiment. A printable copy of our Google Forms survey will be included in the appendix of the resulting publication. Survey respondents will exclusively be students at Brigham Young University that are current members of the Cybersecurity Student Association that choose to compete in the end-of-semester Capture-the-Flag.

Polynomial regression will be performed on the data to establish the relationship between each of the eleven emotions measured in our survey and experience in cybersecurity. Experience in cybersecurity will be measured in two different ways: the number of previous competitions completed and the number of years spent studying cybersecurity, both of which will be self-reported on the survey. Each emotion will be analyzed separately in its relation to both methods of measuring cybersecurity experience so that we may determine which of the predictions of emotional states throughout the ISP accurately relate to the emotions felt, as reported by the subjects. The regression performed on the relationship between experience in cybersecurity and the range of emotions will generate new knowledge of how the levels of each of these emotions vary in respect to experience in cybersecurity education and participation in Capture-the-Flags, and general measures of their likelihoods throughout the process as well.

Pilot Study

In our exploration of this topic, we studied multiple CtFwriteups to get an understanding of what a common thought process of solving a CtF involved. Two writeups that were examined were pulled from public postings on the CTFTime platform (2021). They were published as part of the UIUCTF, by the BYU Cyberia CTF Team. The third was a HackTheBox Ct\TF style question solved and explained by another participant. Appendixes A and B are two of the writeups which we examined.

While examining these writeups, we noticed that often reports could be lumped into two groups: those that focused solely on the submission of the correct path for solving the problem, and those that explained what they tried and what had failed along the way to solve it. This latter group was found to have reported having felt more expressions throughout the problem-solving process. Emotions such as curiosity were most often seen after a new piece of information was discovered. Others such as frustration and disappointment were felt when a certain avenue or strategy did not yield any success. These are a few of the feelings that we desire to explore further in our research and application of the ISP.

To ensure that we have sufficient data to work with in the future, along with hosting our own CtF competition internal to the BYU Cybersecurity Program, the competition will include incentives for well-written writeups to be produced. With aide from a grant provided by the BYU College of Engineering Weidman Center for Global Leadership, we will incentivize writeups with prizes and instructions to include as much affect details as possible.

Limitations

Sampling Biases

Pre-screening. Our sample comes completely from members of the Cybersecurity Student Association at Brigham Young University. This may not be a representative population of cybersecurity students as a whole. In the future, we may expand our competition to include other institutions, thus gaining a wider reach. However, we currently have no plans to address this failing.

Self-selection. Those who choose to compete in competitions may not represent cybersecurity students as a whole. We do not plan to address this failing.

Non-response. The competitors may choose not to take the survey or submit written reports following the competition. We try to combat this by offering incentives through point rewards, but these points may not be enough to convince competitors to participate in the study. To incentivize writeups, we will provide prizes to the top informational submissions.

Survivor. We intend for students to take the survey immediately after they have completed a challenge. This means students who are unable to complete a challenge won't be able to fill out a survey for that specific challenge.

Re-sampling. Our challenges range in difficulty, and surveys are meant to be taken after each challenge. We also expect a correlation between cybersecurity experience and challenges completed. Thus, it seems inevitable that more experienced students will take more surveys.

Other Failings

Sample size. It is possible that, through natural variation within a population, our sample deviates from the norm by a significant amount. This may skew our results unpredictably.

Delineation. We intend for students to take the survey immediately after they have completed a challenge. We suspect some emotions experienced during the challenge may be merged, and forgotten. It would be ideal if each student would constantly report emotions during each challenge, but this would be too tedious and intrusive.

Conclusion

As we dive further into the learning of cybersecurity concepts through the lens of the Information Search Process, within the contexts of Capture-the-Flag competitions, we expect results both along the predicted outcomes, as well as various unknown outcomes. Our overarching hope in performing this research is for three general outcomes. First, an increased understanding of the emotional and intellectual experience of solving a problem, as illustrated by the Information Search Process approach. Second, an increased understanding of how the delivery of a Capture-the-Flag problem affects the learning experience of the participant. Finally, a greater understanding of effective cybersecurity education, in which actionable steps are identified to better teach technical skills and approaches.

References

Center of Academic Excellence in Cybersecurity Community. (2021). Retrieved October 26, 2021, from https://www.caecommunity.org/about-us/what-cae-cybersecurity

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. Proceedings of the International Conference on Security and Management (SAM).

Chothia, T., & Novakovic, C. (2015). An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. 2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15).

CTFtime Team (2021). Retrieved October 26, 2021, from https://ctftime.org.

Harmon, T. D. (2016, September 14). *Cyber Security Capture The Flag (CTF): What Is It?* Cisco Blogs. Retrieved October 26, 2021, from https://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it

Holliday, W. and Li, Q. (2004). Understanding the millennials: updating our knowledge about students to improve library instruction. Reference Services Review, 32(4), 356-366,

Kuhlthau, C. C. (1993). Seeking meaning: a process approach to library and information services. Norwood, NJ: Ablex Press.

Kuhlthau, C. C., Heinström, J., & Todd, R. J. (2008). The 'information search process' revisited: Is the model still useful. *Information research*, *13*(4), paper 355. Retrieved October 26, 2021, from http://InformationR.net/ir/13-4/paper355.html]

Leune, K., & Petrilli Jr, S. J. (2017). Using capture-the-flag to enhance the effectiveness of cybersecurity education. Proceedings of the 18th Annual Conference on Information Technology Education,

McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the flag as cyber security introduction. 2016 49th Hawaii International Conference on System Sciences (HICSS),

Mink, M., & Greifeneder, R. (2010). Evaluation of the offensive approach in information security education. IFIP International Information Security Conference,

Muntean, C. I. (2011). Raising engagement in e-learning through gamification. Proc. 6th international conference on virtual learning ICVL,

National Security Agency. (2021) Retrieved October 26, 2021, from https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

O'Neill, G., & McMahon, T. (2005). Student-centered learning: What does it mean for students and lecturers,

Subhash, S., & Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. *Computers in human behavior*, *87*, 192-206.

Švábenský, V., ˇCeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security, 102. https://doi.org/10.1016/j.cose.2020.102154

APPENDIX A

CtF Writeup: UIUCTF 2021- Chaplin's PR Nightmare 1-8 Writeups

- Type - OSINT
- Points - 50 for 1-7, 88 for 8

Chaplin's PR Nightmare - 1

Description

Charlie Chaplin has gotten into software development, coding, and the like...
He made a company, but it recently came under fire for a PR disaster.
He got all over the internet before he realized the company's mistake,
and is now scrambling to clean up his mess, but it may be too late!!
Find his Twitter Account and investigate! NOTE THAT THESE CHALLENGES DO NOT HAVE DO BE DONE IN ORDER!

The inner content of this flag begins with "pe"

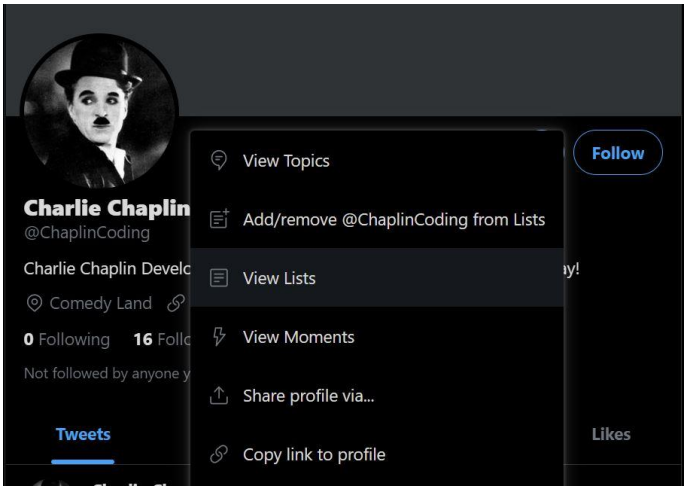
author: Thomas

Writeup

Starting off with the first challenge, we are given a few key pieces of information. First of all, a full name. Next we also have key words such as coding, Software development etc.. These are good to use to modify search parameters to vary a search until the desired result is found.

Thankfully, since they've given us information, and a platform to look on, this should be pretty straight forward. Going to Twitter, we can use the search function and start plugging in the combinations we have. One thing with Twitter searches and other search engines in general, is to sort by the type of content you're looking for to begin with. For this challenge, that would be a profile, instead of a specific tweet or hashtag or trending topic.

So as the above image shows, "charlie chaplin coding" brings up a solitary account - this looks like it. Further investigation leads to a few couple things. First off, there's a YouTube link, which will lead us straight to the next challenge. After looking at a few of the tweets, we can see that he has one thread dedicated to "lists". Any Twitter user who's used it for long enough will know that Twitter users have the ability to create their own "lists", mostly containing users they select for some reason.



Now once we open that we are rewarded with a flag right away. Not too bad, but definitely a good place to hide a flag! A common trend among these challenges is that they show off side features of platforms that require a step or two to discover.

Flag: uiuctf{pe@k_c0medy!}

Real-World Application

When it comes to initial OSINT Challenges and search engines, it helps to utilize a bit of google-fu like skills. Search engines such as Twitter's often include additional filters that can be used to parse through less relevant results. Next, identifying key words to utilize in search parameters and then testing a combination of such parameters will allow for the search to be more accurate and thorough. These combined with other strategies such as including the '@' character or ommitting words or requiring words lead to more optimal searching, which is a necessary tool for cybersecurity.

Chaplin's PR Nightmare - 8 (Extreme)

Description

Straightup doxx Charlie by finding the email he set all these accounts up with, and investigate it.

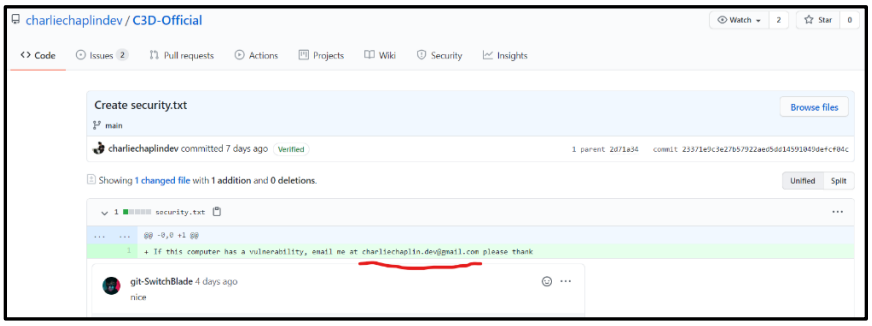
The inner content of this flag begins with "b0"

author: Thomas

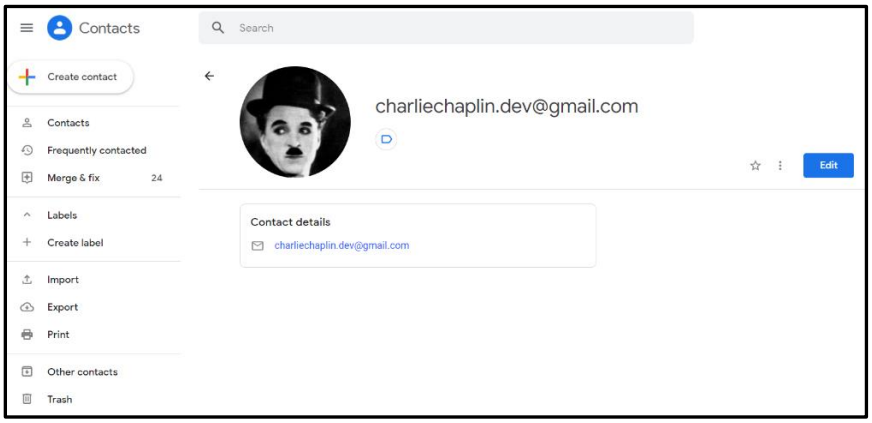
> Hint: This challenge was inspired by something previous.

Writeup

The first step before doing anything else is finding the email. One trick for finding sensitive information in GitHub repos is looking at previous commits - if someone puts sensitive information and then rewrites it, you can access all that info by looking at the history. We had already found Chaplin's GitHub here, so it was a matter of looking around. While looking through the C3D-Official repository commits, we find an email address in the commit titled "Create security.txt". Perfect!



Since it's a Google account, I figured there would be a lot of information about the account that I could see. I opened him in Google Contacts online, but there didn't seem to be anything on there, except a profile picture. I downloaded the photo and ran exiftool on it and such. I didn't find anything particularly useful, and was going to go full steg mode on it until I decided to see what his account connected with first.

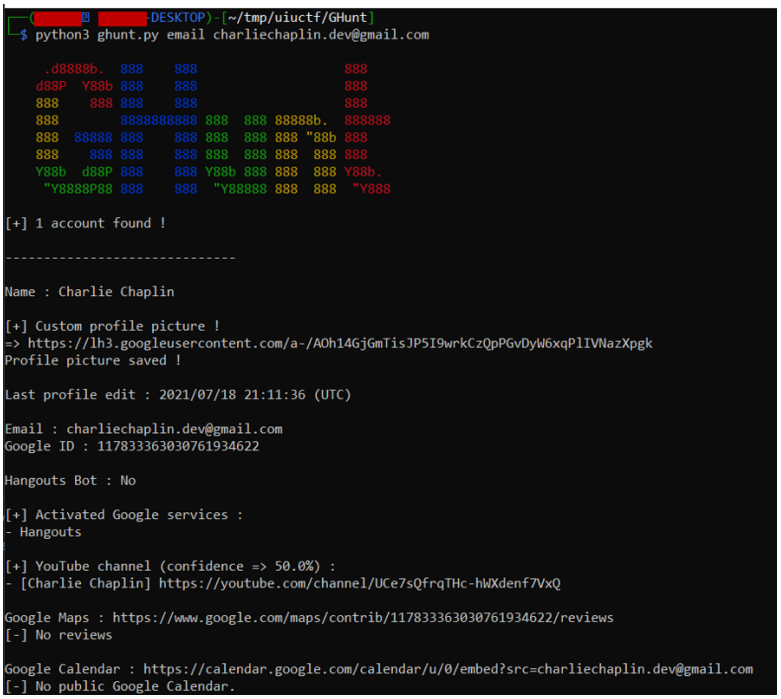


I looked back at the description and decided to do a little digging based on the hint, "This challenge was inspired by something previous". My teammate had already looked around on all the other sites and social media that he was attached to and couldn't find anything, so I decided to look at some of the writeups for OSINT challenges from last year. In a writeup for "Isabelle's Bad Opsec 4" by IrisSec, skat talked about a rabbit hole he went down while searching for the answer - going after the person's Google ID. He explained the implications could include seeing Google Maps reviews, and even put This might make for an interesting future challenge if any potential CTF organizers are reading this (hint hint, nudge nudge). This just seemed to align too perfectly!

I did a Google search for how to connect Gmail accounts to other accounts and came across GHunt. GHunt is a GitHub repository that uses your local Gmail account cookies to find information about a Gmail address, including:

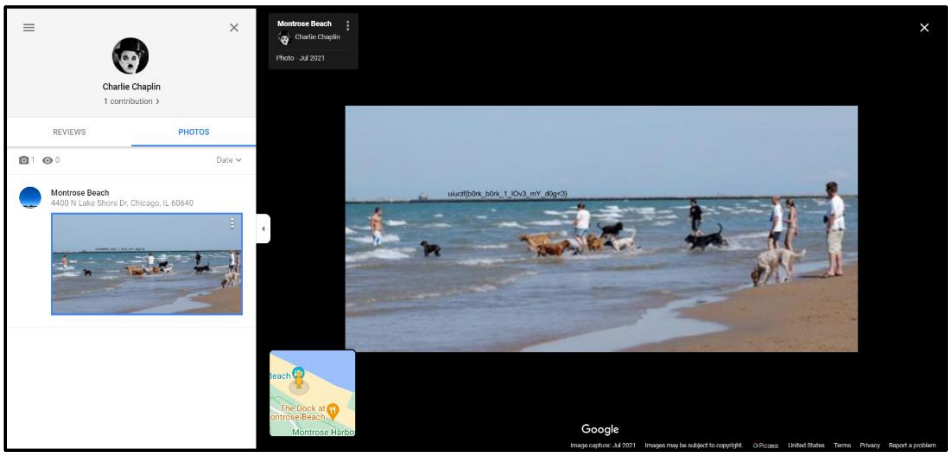
- Owner's name
- Last time the profile was edited
- Profile picture (+ detect custom picture)
- Activated Google services (YouTube, Photos, Maps, News360, Hangouts, etc.)
- Possible YouTube channel
- Google Maps reviews (M)
- Possible physical location (M)
- Events from Google Calendar (C)
- and more!

I cloned the repository, had to install Chrome (since I was on WSL and it kept breaking because it couldn't locate Chrome in the file system), then put the 5 cookies from a fake Google account I set up to run it.



As you can see above, we were given a link to his profile picture (which I already had), a YouTube channel, a Google Maps account, and a Google Calendar. The YouTube channel ended up being a popular Charlie Chaplin channel with millions of subscribers, so I knew it wasn't right. The Google Calendar (supposedly) didn't have any public events, and even though there were no reviews for Google Maps, I went to the link anyway.

When you open the link, you can see Charlie Chaplin has 1 contribution. When you click on photos and open it up, you can see a photo was added in Montrose Beach in Chicago, IL with a flag on it!



Flag: uiuctf{b0rk_b0rk_1_lOv3_mY_d0g<3}

Real-World Application

I think this challenge is a prime example of how one account can link you to other places that you may not suspect. Since this account was fake and set up simply for the purposes of linking to Google Maps reviews, there wasn't much information to see. However, seeing the list of what GHunt can link to you with simply one email can be quite scary - any linked Google services, location history, current location, your calendar, etc. This shows you some of the possible dangers of using a Google account, and some of the avenues to track someone down through OSINT.

Another lesson to learn from this is more CTF-specific, but looking at writeups from previous iterations of a CTF can give you a good insight into how the CTF is run, what types of challenges they may have, and even specific methods that organizers will use from CTF to CTF. The writeup by IrisSec that we've linked to above cracked open the whole case!

APPENDIX B

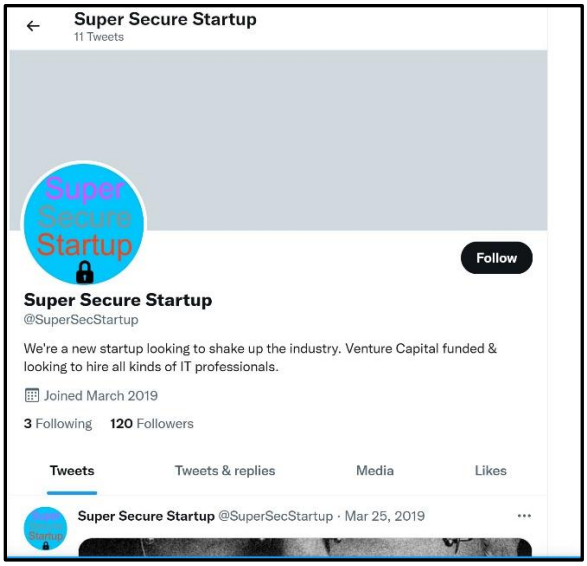
CtF Writeup: HTB: We Have a Leak

Overview

We Have a Leak is an OSINT challenge of medium difficulty on Hack the Box. I chose this challenge as I really enjoy OSINT challenges and the fun that comes with scouring every cornerof the internet in search of information. The user rating seemed to reflect the actual rating as most users found it to be of medium difficulty. I personally found it a bit easier, as I have some experience in OSINT already, but nonetheless some higher level thought went into this challenge.

Technical Walkthrough

This challenge is started by downloading a password protected zip file. The only information thatis given is “Super Secure Startup's private information is being leaked; can you find out how?”. Ibegan with a simple google search of Super Secure Startup. The first result shows us a twitter page: https://twitter.com/supersecstartup?lang=en



This page pretty clearly looks like something for a capture the flag challenge so I knew I was onthe right track. I began clicking on everything and anything I could on the site, looking through photos, comments, and even people who liked the posts. A post that stood out to me was the following:

Let’s take a look at who this JTerranwald is:
https://twitter.com/JTerranwald

Josh Terranwald is a web developer who seems to like youtube and dogs. There is not much herebut I put his profile on the backburner for now.

In the comment section of one of their other posts we see a reply from Johanna Boyce, with her super secure startup email

https://twitter.com/boyce_johanna

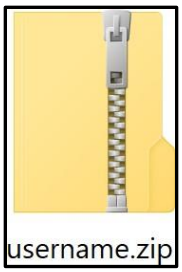
Johanna seems to be the HR Manager at Super Secure Startup and she seems to have posted some rather sensitive data regarding the company, including their office layout and some plansfrom meetings.

The last relevant person I was able to find by scouring the comment section was Bianka Phelps,who had commented on a post about their flagship initiative.

https://twitter.com/BiankaPhelps

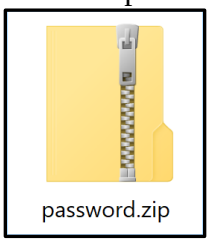
Bianka is an HR professional at Super Secure Startup. Again she has seemed to post some sensitive information about the company including what seems to be a SSH default password onone of their whiteboards. This may be helpful in the future.

Returning to the initial password protected zip file I downloaded, the first password was given tous by hackthebox. Inside the mock_ssh_login directory we have a username.zip directory.

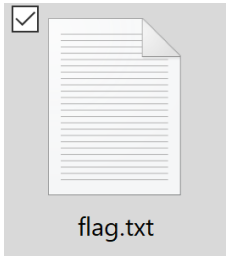


Now I already know a few people who work for Super Secure Startup, Josh Terranwald, JohannaBoyce, and Bianka Phelps. For this zip file I tried various iterations of those names, their full name, their first initial and last name, and finally found that the password was j.terranwald. In that directory we have a password.zip folder.

Now earlier we found a SSH default password on a post from Bianka's whiteboard. Trying SupSecStart#Winter2018! the password just did not work. This seems to be a pretty standard password for the company so I had to do some thinking here. It looks like most if



not all of theposts made by the company and its employees were made in March of 2019. So I tried SupSecStart#Spring2019!. This password ended up working. Within this



directory we had ourflag.txt which contained our HTB flag.

Technical Review

As I stated above I have had some experience with OSINT challenges in the past. While this challenge relied solely on twitter, some OSINT challenges require you to search outside of the most common social media platforms. There was a fairly sketchy website with the same name assuper secure startup and so I felt like it was safe to assume it was not a part of the challenge. If something feels wrong or malicious it will probably not be a part of a challenge. The makers of these challenges do a fairly good job of making it look fake without being malicious.

The number one thing I wish I would have done differently in this challenge was open the zip folder before I started searching. I totally forgot that it was a part of the challenge so I spent quitea bit of time digging through the social media information looking for everything I could. I ended up falling into some rabbit holes that I would not have entered if I would have just been looking for SSH credentials.

These challenges are designed to be difficult but if you are spending more than 15-30 minutes tofind the next piece of information you are probably following a red herring, which is something to be aware of. If you find yourself searching for extended periods of time, take a break and re-evaluate what information you have and what you can use.