Issues in Informing Science + Information Technology

An Official Publication of the Informing Science Institute
InformingScience.org

IISIT.org

Volume 21, 2024

GAMIFIED CYBERSECURITY EDUCATION THROUGH THE LENS OF THE INFORMATION SEARCH PROCESS: AN EXPLORATORY STUDY OF CAPTURE-THE-FLAG COMPETITIONS

[RESEARCH-IN-PROGRESS]

Albert Tay*	Brigham Young University, Provo, UT, USA	albert_tay@byu.edu
Sebastian Hayes	Brigham Young University, Provo, UT, USA	sh933@byu.edu
Drew Wilson	Brigham Young University, Provo, UT, USA	aw053102@byu.edu
Emmie Hall	Brigham Young University, Provo, UT, USA	elhall279@gmail.com
Dallin Kaufman	Brigham Young University, Provo, UT, USA	kaufman1@byu.edu

* Corresponding author

ABSTRACT

Aim/Purpose	Capture the Flag (CTF) 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.
Background	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 takes. 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 aims to investigate the learning of cybersecurity

Accepted by Editor Eli Cohen | Received: December 16, 2023 | Revised: February 6, 2024 | Accepted: February 12, 2024.
Cite as: Tay, A., Hayes, S., Wilson, D., Hall, E., & Kaufman, R. (2024). Gamified cybersecurity education through the lens of the information search process: An exploratory study of Capture-the-Flag competitions [Research in progress]. *Issues in Informing Science and Information Technology, 21,* Article 1.
https://doi.org/10.28945/5313

	concepts within the framework of the ISP, specifically in the context of CTF competitions.
Methodology	A comprehensive research methodology designed to incorporate quantitative and qualitative analyses to draw the parallels between the participants' emotional experiences and the affective dimensions of learning will be implemented to measure the three primary goals.
Contribution	This study contributes significantly to the broader landscape of cybersecurity education and cognitive-emotional experiences in problem-solving.
Findings	The study has three primary goals. First, we seek to enhance our understanding of the emotional and intellectual aspects involved in problem-solving, as demonstrated by the ISP approach. Second, we aim to gain insights into how the presentation of CTF challenges influences the learning experience of participants. Lastly, we strive to contribute to the improvement of cybersecurity education by identifying actionable steps for more effective teaching of technical skills and approaches.
Recommendations for Practitioners	Competitions reinforce and teach problem-solving skills applicable in various technical and non-technical environments outside of the competitions.
Recommendations for Researchers	The Information Search Process (ISP) framework may enhance our understanding of the emotional and intellectual aspects involved in problem-solving as we study the emotional ties connected to each step an individual takes as the individual goes through the problem-solving process.
Impact on Society	Our pursuit of advancing our understanding of cybersecurity education will better equip future generations with the skills and knowledge needed to address the evolving challenges of the digital landscape. This will better prepare them for real-world challenges.
Future Research	Future studies would include the development of a cybersecurity curriculum on vulnerability exploitation and defense. It would include practice exploiting practical web and binary vulnerabilities, reverse engineering, system hardening, security operations, and understanding how they can be chained together.
Keywords	cybersecurity, Capture-the-Flag, information search process, gamification

INTRODUCTION

In the ever-evolving landscape of information acquisition, protection, and learning, Carol Kuhlthau's ISP (Information Search Process), crafted in 1993, stands as a pivotal framework for comprehending the intricate journey undertaken by researchers as they delve into the depths of their chosen subjects. The ISP consists of six stages, which are the following:

1. Task Initiation
2. Topic Selection
3. Exploration
4. Focus Formulation
5. Information Collection
6. Search Closure

Her seminal work illuminates the profound emotional dimensions intertwined with each step of this scholarly expedition. As researchers embark on the voyage of studying their selected topics or arguments, a discernible transition unfolds, guiding them from the realms of uncertainty into the clarity

of knowledge acquisition. Kuhlthau (1993) further elucidates that in the pursuit of knowledge, the learner's feelings, thoughts, and actions are profoundly interconnected.

Central to the research process, uncertainty and doubt emerge as formidable adversaries, frequently obstructing the path to knowledge. Kuhlthau's (1993) seminal work adeptly addresses the multifaceted nature of uncertainty, emphasizing the pivotal nature of the transition from doubt to certainty within the search process. Positioned within this framework, researchers gain a profound insight into their progress along the ISP. This understanding empowers them to navigate the turbulent waters of negative emotions that often accompany the learning experience, paving the way for the cultivation of joy and accomplishment in the pursuit of knowledge.

Over the years, since its conceptualization in the late 1980s and early 1990s, Kuhlthau's (1993) ISP has undergone rigorous scrutiny and refinement. In 2008, Kuhlthau and her associates at Rutgers University revisited their pioneering work on the ISP. This reevaluation became necessary due to the rapid advancements in technology that had unfolded over this period. It was imperative to ascertain whether the ISP model retained its effectiveness in evaluating learning in today's digitally-driven educational landscape. A comprehensive study that revisited the findings of ISP yielded a resounding endorsement, affirming that the ISP, as a model, continued to serve as a valuable theoretical and explanatory framework for user studies in librarianship and information science (Kuhlthau et al., 2008).

In the realm of education, particularly in an increasingly digital environment, researchers recognized the need to assess the applicability of the ISP model. With readily accessible information at their fingertips, there was an expectation that the learning process would become more streamlined. However, the evidence gathered thus far has shed light on a different reality. The ISP remains highly relevant in the digital age, dispelling the notion that abundant access to information translates into a simpler quest for knowledge (Holliday & Li, 2004). Building upon the insights gained from revisiting the ISP, it is evident that this model persists as a valuable tool, intricately connecting the progression of emotions and cognitive responses to the learning journey. It serves as an indispensable guide for researchers in their relentless quest for information.

The ISP Model may be utilized to improve cybersecurity education. In 1999, the National Security Agency (NSA) initiated the Center of Academic Excellence in Information Assurance Education (CAE-IAE) program (NSA, 2022). This groundbreaking program offered institutions the coveted CAE-IAE designation upon successfully meeting rigorous curriculum and program requirements. Under the stewardship of the NSA's National Cryptologic School, the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program was born. With a consortium of federal partners, including the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST), the National Initiative on Cybersecurity Education (NICE), the National Science Foundation (NSF), the Department of Defense Office of the Chief Information Officer (DoD-CIO), and US Cyber Command (USCYBERCOM), the NCAE-C program has burgeoned to encompass over 300 institutions across the nation, spanning designations in Cyber Defense (CAE-CD), Cyber Research (CAE-R), and Cyber Operations (CAE-CO) (Center of Academic Excellence in Cybersecurity Community, 2022; National Security Agency, 2022).

In the expansive realm of cybersecurity education, an abundance of resources has been dedicated to fostering the acquisition and development of relevant skills. Amid this vast landscape lies a distinctive domain: cybersecurity Capture The Flag (CTF) competitions. These competitions serve as trials for various technical cybersecurity challenges, demanding participants to unravel complex conundrums within tight time constraints. Challenges are presented as problems, accompanied by prompts, and are solved by submitting unique text phrases called flags found upon completion of these challenges. These enigmatic challenges span a diverse array of topics, encompassing web vulnerabilities, cryptography, reverse engineering, Open Source Intelligence (OSINT), and more. Beyond the adrenaline-

fueled contest, participants often culminate their experience by submitting comprehensive written reports detailing their solutions to these cerebral challenges (Harmon, 2016).

The educational value of CTF competitions within the cybersecurity domain is not a recent phenomenon. Dating back to 1996, these competitions have served as dynamic educational exercises, offering immersive experiences with specific technologies and subjects while concurrently fostering a holistic understanding of cybersecurity topics (Švábenský et al., 2021). CTF competitions are instrumental in nurturing problem-solving skills that transcend disciplinary boundaries, finding practical applications in technical and non-technical domains (Leune & Petrilli, 2017; McDaniel et al., 2016; Tan & Ouh, 2021). This pedagogical methodology, fueled by gamified elements, has proven highly effective in imparting technical skills and topics to students.

However, within this expansive landscape, an intriguing avenue remains uncharted – the nuanced emotions and processes that students encounter throughout CTF competitions. It is within this unexplored territory that we see the ISP, as revisited and refined by Kuhlthau (2004), as an optimal framework for investigation.

> *Research Hypothesis:* The ISP offers a pertinent and potent framework for evaluating the effectiveness of CTF competitions in cybersecurity education, primarily due to its intrinsic focus on the cognitive and emotional experiences that permeate the learning journey.

By employing the ISP model to assess students' emotions during CTF challenges, we aspire to achieve a deeper understanding of several critical facets:

- The validity of the ISP as a robust tool for evaluating the challenges presented by CTF competitions.
- The efficacy of CTF competitions as vehicles for imparting cybersecurity education.
- The identification of areas for improvement within the realm of CTF challenges is discerned through the lens of the ISP.

As we embark on this study expedition, we anticipate unveiling a richer tapestry of emotions and experiences that shape the world of cybersecurity education, setting the stage for a more informed and emotionally resonant pedagogical landscape.

LITERATURE REVIEW

In our quest to explore the applicability of the ISP to cybersecurity education through CTF activities, we conducted an extensive examination of the existing body of literature. Our diligent review involved categorizing articles based on the underlying themes of their research inquiries. This exhaustive exploration unearthed critical commonalities spanning the domains of education, gamification, and the broader realm of CTF competitions. Our overarching objective is to craft a robust study that delves into the intricate relationship between the ISP and the dynamic landscape of CTF competitions.

CTF activities, renowned for their competitive nature, serve as a potent showcase of participants' technical prowess. Yet, these activities transcend mere contests; they offer a fertile ground for the acquisition and application of new skills in the realm of cybersecurity. Existing studies illuminate the profound impact of competitions and challenges, particularly when they compel students to collaborate and employ their knowledge. These experiences culminate in the enhancement of students' technical proficiency, a heightened level of interest in the subject matter, and a unique ability to disseminate their newfound expertise (Cheung et al., 2011; Deaconescu et al., 2022). This empirical evidence portends a promising outlook, as a student's capability to teach a subject they have learned is a compelling indicator of advanced comprehension.

Subhash and Cudney (2018), in their exploration of gamified learning, provide further testament to the pedagogical potential of gamification in higher education. Their findings underscore the

transformative impact of gamified learning and teaching systems, emphasizing their potential to elevate student engagement, motivation, and overall academic performance. The successful integration of gamification and game-based learning emerges as a beacon of promise for the realm of higher education.

CTF competitions, often conducted as team events, compel student competitors to apply their preexisting knowledge in novel and inventive ways. They are also required to learn and apply new knowledge gained during the CTF. These aspects align CTF activities with the tenets of Challenge-Based Learning, a pedagogical approach that empowers students to harness their existing knowledge and new knowledge in the pursuit of creative solutions. Concurrently, research investigating curricula underpinned by Student-Centered Learning principles highlights the profound impact of affording students a high degree of choice and involvement in shaping their educational journeys (Deaconescu et al., 2022; O'Neill & McMahon, 2005). This autonomy begets heightened motivation and satisfaction with the educational process. Notably, academic game-like competitions such as CTF imbue students with precisely this high degree of choice, promising to bolster motivation and satisfaction throughout the learning voyage.

Within the broader context of enhancing our comprehension of students' cognitive experiences in education, Carol Kuhlthau's ISP emerges as a beacon of insight. This six-stage model, as shown in Figure 1, which encapsulates the holistic journey of information-seeking, adds a valuable layer of understanding by acknowledging the interconnected realms of affective (feelings), cognitive (thoughts), and physical (actions) experiences in the process of acquiring new knowledge. The six stages people go through when seeking information are:

1. Initiation: Feeling uncertain, individuals recognize the need for information.
2. Selection: They start exploring their topic and formulating a general idea.
3. Exploration: Actively search for information, delving deeper into the topic.
4. Formulation: Crystalize their ideas, refine research questions, and develop a structured approach.
5. Collection: Actively gather relevant information.
6. Presentation: Synthesize and present findings or research outcomes.

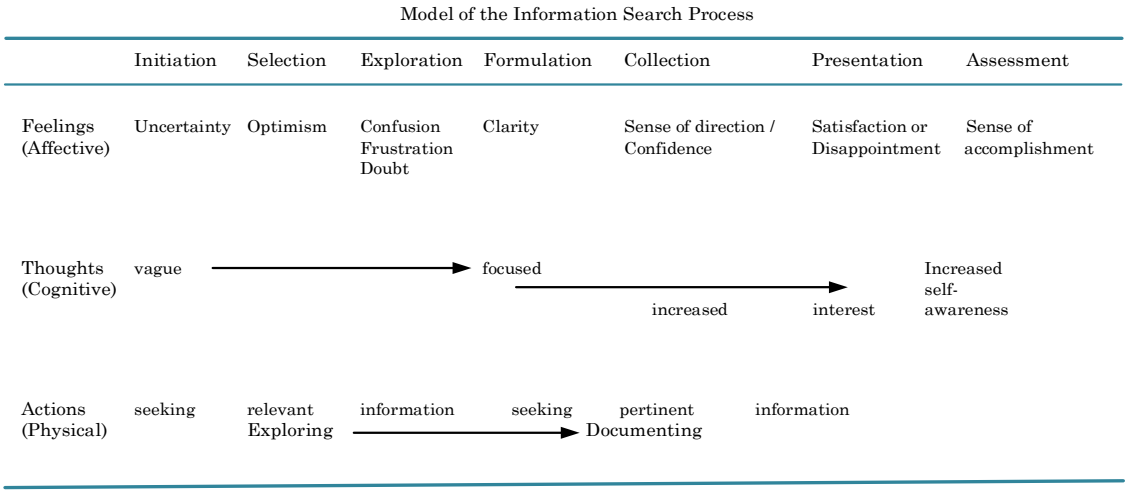


Figure 1. Model of the information search process (Kuhlthau, 2004, p. 82)

The model emphasizes the emotional and cognitive aspects of information-seeking, understanding that feelings like uncertainty and confusion are part of the process, impacting the overall experience and outcomes.

Kuhlthau's (1993) research underscores a pivotal finding: the primary objective of information seeking is not merely the collection of information as an end in itself but rather the accomplishment of the task that instigated the search. In this context, CTF competitions offer an additional wellspring of intrinsic motivation, further reinforcing students' commitment to their practical education. Kuhlthau et al.'s (2008) later research corroborates the notion that students who grapple with the learning process, experiencing challenges and struggles, ultimately attain a deeper well of knowledge and heightened confidence. Furthermore, heightened engagement with course material culminates in more positive emotions at the journey's conclusion. Collectively, these findings paint a vivid picture of the potential to enhance education by nurturing student motivation, critical thinking, and the practical application of knowledge.

As CTF competitions represent a gamified method for showcasing cybersecurity skills, a survey of literature on gamification becomes an indispensable resource. Studies in this domain underscore the capacity of gamification to inject enjoyment and engagement into the learning process without compromising instructional credibility (Muntean, 2011). Subhash and Cudney's (2018) work underscores the emotionally charged dimension of game-based learning, illuminating how it fosters feelings of focus, engagement, accomplishment, productivity, and motivation among players. Additionally, games are shown to yield improvements in knowledge acquisition, content mastery, learner motivation, and academic effort. These insights unequivocally affirm that the inclusion of gamified elements within the learning process begets an array of positive emotional outcomes.

Current US and global trends show that there is a shortage of qualified cybersecurity professionals, which the gamified elements of CTFs can address. The ISACA's 2022 State of Cybersecurity report stated that 62% of organizations' cybersecurity teams were somewhat or significantly understaffed, and 47% of organizations reported a 3-6-month process to hire qualified candidates. Both reported percentages have increased in the past two years (ISACA, 2022). One of the main challenges in filling positions has become the lack of qualified applicants. The realization of this problem does not solely lie with employers – students are noticing that they are not receiving the skills necessary for employment in their university cybersecurity education.

Further refining our focus, we narrowed our literature survey to scrutinize findings related specifically to CTF competitions. These exercises, typically oriented towards offensive cybersecurity education, yield substantial gains in the understanding of network vulnerabilities. In a notable ANOVA test, participants in CTF competitions demonstrated a statistically significant higher comprehension of network vulnerabilities compared to their counterparts in defensive-only courses (Mink & Greifeneder, 2010). These findings mirror our earlier observations in the broader gamification category, reiterating that cybersecurity challenges, including CTF, catalyze motivation for learning, foster enjoyment in the learning process, engender satisfaction in achievement, and augment practical knowledge (Chothia & Novakovic, 2015). Moreover, CTF activities cultivate students' confidence in their abilities (Leune & Petrilli, 2017), a critical facet of their educational journey. Notably, student motivation surfaces as a pivotal predictor of educational outcomes, underscoring its far-reaching implications (McDaniel et al., 2016). A comprehensive exploration also reveals that participants who explore a diverse array of challenges, aligning their choices with their interests, tend to learn more effectively – an outcome that adds a layer of richness to the educational landscape.

CTF competitions constitute a potent vehicle for the practical application of acquired knowledge, offering a clear trajectory for future studies – both indispensable components of effective learning. Furthermore, the gamified environment intrinsic to CTF activities serves as a catalyst for heightened student interaction with course material, kindling motivation, and fostering overall satisfaction with the learning journey. This amalgamation of insights converges to underscore the profound potential of CTF competitions as a transformative force in the realm of cybersecurity education.

METHODOLOGY

This study endeavors to establish the utility of the ISP model in assessing emotional experiences during information gathering and its relevance as a framework for evaluating the effectiveness of CTF competitions in cybersecurity education. To achieve this, a comprehensive research methodology has been designed, incorporating both quantitative and qualitative analyses to draw parallels between emotions experienced during information gathering (as delineated in the ISP) and the affective dimensions of learning cybersecurity skills in CTF competitions. The primary data sources for this study are the CTF writeups, observations of the participants, and surveys. This study will be conducted collaboratively by the Brigham Young University (BYU) Cybersecurity Research Lab and the Cybersecurity Student Association of BYU, specifically centered around their end-of-semester CTF event.

To substantiate our hypothesis, a dual-pronged approach will be adopted. First, a thematic analysis will be performed using the grounded theory approach to identify common themes from the CTF writeups: "It is often observed that no cookbook or recipe exists for qualitative research… we view qualitative data as an ingredient, like flour, that can be used in a creative and wide-ranging variety of ways" (Graebner et al., 2012, p. 276). To aid in the thematic analysis, multiple coders will evaluate the writeups produced by the participants. Cohen's kappa coefficient will be used as the main metric for quantifying inter-rater agreement beyond chance in theme-based qualitative analysis. By employing Cohen's kappa coefficient, we will be able to quantify the degree of agreement among coders, identify areas of discrepancy, and refine coding protocols to enhance consistency and reliability. Additionally, a longitudinal survey will be conducted to gauge the evolving attitudes of participants toward the field of cybersecurity as their experience in the domain progresses. This methodology is chosen for its suitability in evaluating complex emotional processes – a common analytical approach in studies with comparable hypotheses.

The emotions under scrutiny encompass uncertainty, optimism, confusion, frustration, doubt, sense of direction, clarity, confidence, satisfaction, disappointment, and accomplishment. These emotional facets are aligned with those identified in the ISP model. The data collection process will involve the administration of a survey utilizing a 5-point Likert scale, where respondents rate their agreement with statements framed around emotional experiences during the CTF challenges. The Likert scale ranges from 1, indicating "strongly disagree," to 5, signifying "strongly agree," with a midpoint at 3, representing neutral sentiment. For transparency and reference, a printable version of the survey is included in Appendix A. Survey participants will exclusively comprise students at BYU who have chosen to partake in the End-of-Semester Capture-the-Flag event.

Follow-up evaluations at regular intervals, such as one week, one month, six months, and one year post-intervention, are crucial for understanding the long-term impact of the intervention on participants' knowledge gains, mindset shifts, areas for improvement, and additional learning needs. However, conducting these evaluations also entails considerations related to participant privacy, consent, and ethical adherence.

All data collected will comply with Institutional Review Board (IRB) requirements, and all participants will be assigned a unique participant number. All personally identifiable data, including name, address, contact information, and any other identifying details, will be securely stored separately from the research data, will be encrypted at rest, and will only be accessible to authorized personnel. In capturing sensitive student cognition and emotional data, particularly in educational settings, the IRB requirements become crucial to ensure ethical adherence and participant privacy protection.

Subsequently, regression analysis (multivariate analysis of variance, MANOVA) will be employed to ascertain the relationship between the eleven emotions measured in the survey and participants' cybersecurity experience. We hope to conduct longitudinal studies using MANOVA, which would be a robust and insightful approach to measure the effect of the ISP within the context of CTF

cybersecurity education. It allows for a comprehensive examination of changes over time, contributing valuable insights to both theory and practice.

The quantification of cybersecurity experience will occur through two distinct self-reported measures: the number of previous competitions completed, and the number of years spent studying cybersecurity. Each emotion will be subjected to individual analysis in relation to both methods of measuring the cybersecurity experience. This comprehensive regression analysis aims to identify the emotions that most accurately correlate with the emotions predicted throughout the ISP model and as reported by the study's subjects. The insights derived from this regression analysis and the writeups will contribute to an enhanced understanding of how emotional states vary concerning experience in cybersecurity education, participation in CTF competitions, and general indications of emotional likelihoods throughout the process.

Pilot Study

As part of our preparatory work, we conducted a pilot study to gain insight into the common thought processes employed by participants when solving CTF challenges. The pilot study entailed the examination of multiple CTF writeups, which provided valuable context and preliminary data for our study. Specifically, we reviewed two writeups obtained from public postings on the CTFTime platform (CTF, 2021), which were authored by the BYU Cyberia CTF Team as part of the UIUCTF, and a third writeup that detailed the resolution of a HackTheBox CTF-style question by another participant. Appendices B and C of our study material encapsulate these writeups.

During the analysis of these writeups, an intriguing pattern emerged. Reports could generally be categorized into two distinct groups: one group primarily focused on the submission of the correct path for solving the challenge, while the other elaborated on the strategies attempted and the failures encountered in their quest to conquer the challenge. Interestingly, the latter group reported experiencing a more diverse range of emotions throughout the problem-solving process. Emotions such as curiosity were frequently noted upon the discovery of new information, while frustration and disappointment were prevalent when certain avenues or strategies failed to yield success. These findings underscored the significance of exploring these emotions in our study and applying the ISP model to analyze them.

To ensure an ample volume of data for future analysis and in line with our commitment to enhancing the CTF community, we have planned to host the CTF competition within the BYU Cybersecurity Program. To encourage the production of well-written writeups, we have secured support from the BYU College of Engineering Weidman Center for Global Leadership, which will provide grants, prizes, and instructions to incentivize participants to include rich, effective details in their reports.

Limitations

While our research methodology is robust, it is essential to acknowledge certain limitations inherent to our study. These limitations encompass sampling biases, potential issues related to self-selection, non-response, survivorship bias, sample size considerations, and the challenge of delineating emotions experienced during complex problem-solving processes. These limitations are important to recognize, as they may impact the generalizability and scope of our findings. The limitations of the study are as follows:

Sampling Biases: Our study exclusively relies on participants from the Cybersecurity Student Association at BYU. This may not represent the broader population of cybersecurity students. While there is a potential to expand to other institutions in different regions and hold public CTFs, in the future, this limitation persists in the present study.

Self-Selection: Participants who opt to compete in cybersecurity competitions may not be fully representative of all cybersecurity students, introducing potential biases.

NON-RESPONSE: Despite offering incentives, some participants may choose not to take the survey or submit written reports following the competition, potentially affecting the completeness of our dataset.

SURVIVORSHIP: The timing of our survey, immediately after challenge completion, means that students who are unable to complete a challenge will not be able to provide survey responses for that specific challenge, potentially skewing the data.

RE-SAMPLING: As the difficulty of our challenges varies, and surveys are designed to be taken after each challenge, we anticipate that more experienced students will take more surveys, potentially influencing our results.

SAMPLE SIZE: There is a possibility that natural variation within our sample could deviate significantly from the norm, potentially introducing unpredicted biases into our results.

DELINEATION: We anticipate that emotions experienced during challenges may sometimes overlap or be forgotten, as reporting emotions constantly during each challenge would be impractical and intrusive.

DEMOGRAPHIC DATA: We do not currently capture data relating to age, gender, or native language. Given the limited sampling size for the initial study, these factors will have little to no effect on the outcome but will be considered in future studies as the sample size increases.

ONLINE VS. IN-PERSON PARTICIPATION: The majority of students participate in CTFs remotely by themselves or in small groups in person. The initial study was performed using an individual CTF where participants had to work alone and chose to participate online or in person. The effect of this variable change will be introduced in future studies.

These limitations will be kept in mind during the analysis and interpretation of our findings, and we acknowledge the need for further studies to build upon our work and address these constraints in more extensive studies.

CONCLUSION

As we delve deeper into the realm of cybersecurity education, exploring the intricacies of learning cybersecurity concepts through the lens of the ISP within the dynamic environment of Capture-the-Flag (CTF) competitions, we anticipate that our study will yield a multifaceted set of outcomes. These outcomes encompass not only the anticipated results but also various unforeseen discoveries that may enrich our understanding of this complex domain. In summation, our overarching aspiration in conducting this study extends to three broad objectives, each of which contributes significantly to the broader landscape of cybersecurity education and cognitive-emotional experiences in problem-solving.

INCREASED UNDERSTANDING OF EMOTIONAL AND INTELLECTUAL EXPERIENCES

The foremost objective of our study is to contribute to a heightened comprehension of the emotional and intellectual dimensions inherent in the process of solving complex problems, as exemplified by the ISP framework. By meticulously examining the emotional journey of participants in CTF competitions, we aim to shed light on the intricate interplay between feelings, thoughts, and actions during the pursuit of cybersecurity knowledge. We aspire to unravel the intricate tapestry of emotions – ranging from uncertainty and curiosity to clarity and accomplishment – that students experience throughout the learning process. This deeper insight into the emotional and cognitive facets of

problem-solving is poised to enrich our knowledge of how learners engage with and navigate the challenges of cybersecurity education.

Enhanced Understanding of Delivery Impact in CTF Learning

A second critical objective of our study is to foster an enhanced understanding of how the delivery of CTF challenges shapes the learning experience of participants. CTF competitions represent a dynamic and gamified approach to cybersecurity education, and we seek to unravel the intricacies of how the presentation of challenges influences learners' engagement, motivation, and overall educational outcomes. By dissecting the affective and cognitive responses of participants as they confront CTF problems, we aspire to uncover valuable insights into the efficacy of this pedagogical approach. These findings can inform educators, curriculum designers, and cybersecurity trainers about the nuances of delivering content in a way that maximizes students' learning experiences and outcomes.

Advancing Effective Cybersecurity Education

The third and overarching goal of our study endeavors to advance the realm of effective cybersecurity education. In this pursuit, we aspire to identify actionable steps that can enhance the pedagogy of teaching technical skills and approaches in cybersecurity. By delving into the emotional and cognitive aspects of learning within the CTF context, we aim to offer tangible recommendations and best practices for educators and institutions engaged in cybersecurity education. Our study seeks to bridge the gap between theoretical knowledge and practical application, ultimately contributing to the development of more effective teaching methods and curricula in the field of cybersecurity.

In conclusion, our study into the confluence of the ISP model, cybersecurity education, and CTF competitions is driven by a profound commitment to expanding our collective understanding of the intricate processes underlying problem-solving and learning experiences. We are poised to uncover valuable insights that not only illuminate the emotional and intellectual facets of learning but also inform pedagogical practices in cybersecurity education. As we venture further into this terrain, we remain optimistic that our study will not only fulfill its intended objectives but also inspire further exploration, innovation, and refinement in the realm of cybersecurity education. Ultimately, our pursuit is grounded in the belief that by advancing our understanding of these domains, we can better equip future generations with the skills and knowledge needed to address the evolving challenges of the digital landscape.

References

Capture The Flag (CTF). (2021). *CTF time.* https://CTFtime.org

Center of Academic Excellence in Cybersecurity Community (CAECC). (2022). *What is a CAE in cybersecurity?* https://www.caecommunity.org/about-us/what-cae-cybersecurity

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

Chothia, T., & Novakovic, C. (2015). *An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education.* Paper presented at USENIX Summit on Gaming, Games, and Gamification in Security Education, Washington, United States.

Deaconescu, R. A., Baltoiu, A., Georgescu, T., & Puncioiu, A. (2022). Using Cybersecurity Exercises as Essential Learning Tools in Universities. *International Conference on Computer Supported Education.* https://doi.org/10.5220/0010994700003182

Graebner, M. E., Martin, J. A., & Roundy, P. T. (2012). Qualitative data: Cooking without a recipe. *Strategic Organization, 10*(3), 276-284. https://doi.org/10.1177/1476127012452821

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

Holliday, W., & Li, Q. (2004). Understanding the millennials: updating our knowledge about students to improve library instruction. *Reference Services Review*, *32*(4), 356-366. https://doi.org/10.1108/00907320410569707

ISACA. (2022). *State of cybersecurity 2022 global update on workforce efforts and resources.* https://www.isaca.org/resources/reports/state-of-cybersecurity-2022

Kuhlthau, C. C. (1993). *Seeking meaning: A process approach to library and information services.* Ablex Press.

Kuhlthau, C. C. (2004). *Seeking meaning: A process approach to library and information services* (2nd ed.). Libraries Unlimited.

Kuhlthau, C. C., Heinström, J., & Todd, R. J. (2008). The 'information search process' revisited: Is the model still useful. *Information Research*, *13*(4), Article 355. http://InformationR.net/ir/13-4/paper355.html

Leune, K., & Petrilli, S. J. (2017). Using capture-the-flag to enhance the effectiveness of cybersecurity education. *Proceedings of the 18th Annual Conference on Information Technology Education* (pp. 47-52). ACM. https://doi.org/10.1145/3125659.3125686

McDaniel, L., Talvi, E., & Hay, B. (2016, January). Capture the flag as cyber security introduction. *Proceedings of the 49th Hawaii International Conference on System Sciences, Koloa, HI, USA,* 5479-5486. https://doi.org/10.1109/HICSS.2016.677

Mink, M., & Greifeneder, R. (2010). Evaluation of the offensive approach in information security education. In K. Rannenberg, V. Varadharajan, & C. Weber (Eds.), *Security and privacy – silver linings in the cloud* (pp. 203-214). Springer. https://doi.org/10.1007/978-3-642-15257-3_18

Muntean, C. I. (2011). Raising engagement in e-learning through gamification. *Proceedings of the 6th International Conference on Virtual Learning*, 323-329.

National Security Agency. (2022). *National Centers of Academic Excellence in Cybersecurity.* 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? In G. O'Neill, S. Moore, & B. McMullin (Eds.), *Emerging issues in the practice of university learning and teaching* (pp. 30-39). AISHE.

Subhash, S., & Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. *Computers in Human Behavior*, *87*, 192-206. https://doi.org/10.1016/j.chb.2018.05.028

Švábenský, V., ˇCeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, *102*, 102154. https://doi.org/10.1016/j.cose.2020.102154

Tan, K. H., & Ouh, E. L. (2021, October). Lessons learnt conducting capture the flag cybersecurity competition during COVID-19. *Proceedings of the IEEE Frontiers in Education Conference, Lincoln, NE, USA.* https://doi.org/10.1109/FIE49875.2021.9637404

APPENDIX A
PARTICIPANT QUESTIONNAIRE

IRB Number: **Form number: _____**

Instructions - Part 1

Fill in the following information.

1. **Name: _____**
2. **Challenge Completed:** What challenge did you just complete? (e.g., Challenge 1)

   _____

3. **CTFs Completed:** How many Capture The Flags (CTFs) have you completed prior to this one? _____
4. **Current Semester:** What semester of school are you currently in? (1-10)

   _____

5. **Study Duration:** Estimate the number of months you have spent studying/been interested in cybersecurity. _____

Instructions - Part 2

The following questions ask you to report how strongly you felt each of the emotions listed. You can think of it as asking, "While attempting to solve this challenge, I felt the emotion of _____." Please rate the following statements on a scale from 1 to 5, where:

1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree

6. **Uncertainty: _____**
7. **Optimism: _____**
8. **Confusion: _____**
9. **Frustration: _____**
10. **Doubt: _____**
11. **Having a Sense of Direction: _____**
12. **Clarity: _____**
13. **Confidence: _____**
14. **Satisfaction: _____**
15. **Disappointment: _____**
16. **Accomplishment: _____**

APPENDIX B
CTF WRITEUPS

UIUCTF 2021 – Chaplin's PR Nightmare 1 and 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 TO BE DONE IN ORDER!

The inner content of this flag begins with "pe."

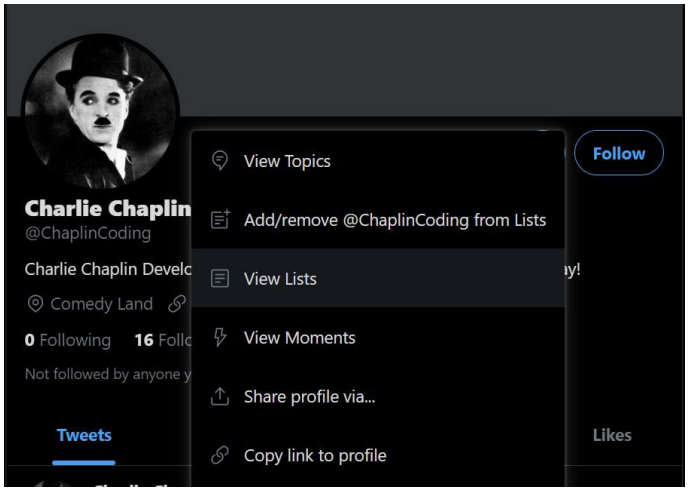
Author: Thomas

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 keywords 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 straightforward. 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, 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 omitting 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.

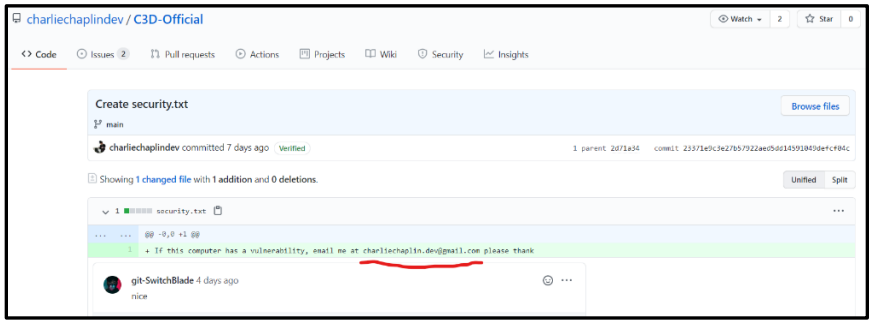
The inner content of this flag begins with "b0"

author: Thomas

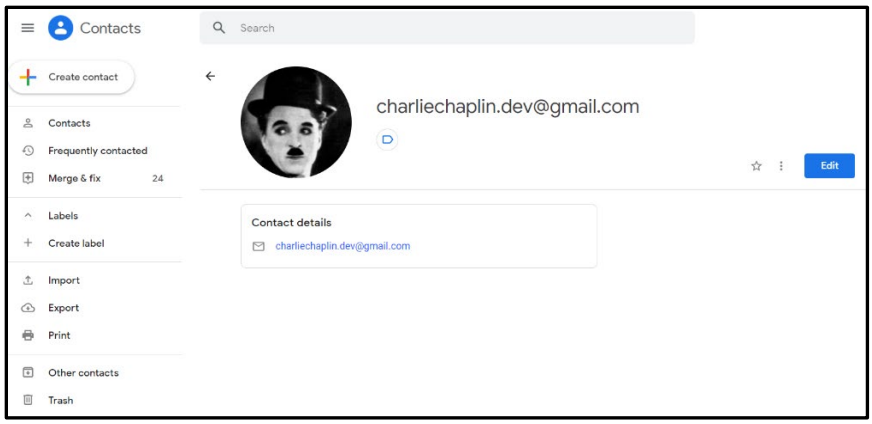
> Hint: This challenge was inspired by something previous.

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 Iris-Sec, 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:

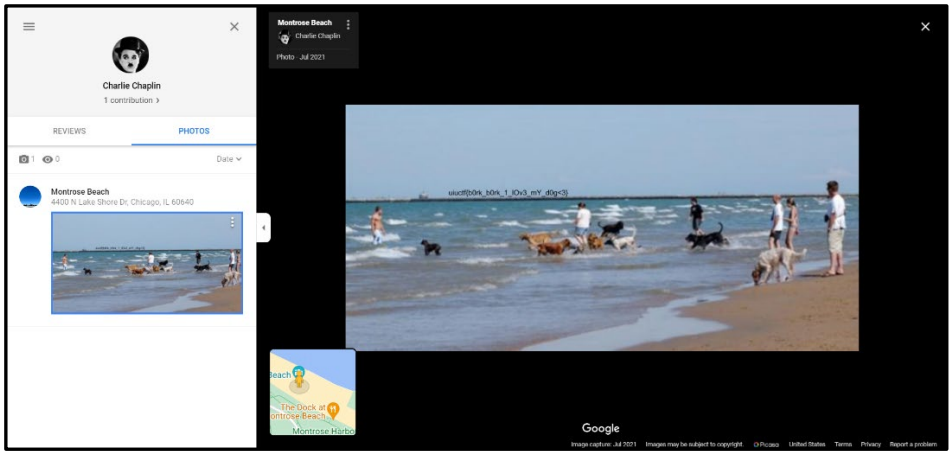
- Owner's name
- Last time the profile was edited
- Profile picture (+ detect custom picture)
- Activated Google services (YouTube, Photos, Maps, News360, Hangouts, etc.)
- Possible YouTube channel
- Google Maps reviews (M)
- Possible physical location (M)
- Events from Google Calendar (C)
- and more!

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.

```
┌──([redacted]@[redacted]-DESKTOP)-[~/tmp/uiuctf/GHunt]
└─$ python3 ghunt.py email charliechaplin.dev@gmail.com

    .d8888b.  888    888                  888
   d88P  Y88b 888    888                  888
   888    888 888    888                  888
   888        8888888888 888  888 88888b.  888888
   888  88888 888    888 888  888 888 "88b 888
   888    888 888    888 888  888 888  888 888
   Y88b  d88P 888    888 Y88b 888 888  888 Y88b.
    "Y8888P88 888    888  "Y88888 888  888  "Y888

[+] 1 account found !

----------------------------

Name : Charlie Chaplin

[+] Custom profile picture !
=> https://lh3.googleusercontent.com/a-/AOh14GjGmTisJP5I9wrkCzQpPGvDyW6xqPlIVNazXpgk
Profile picture saved !

Last profile edit : 2021/07/18 21:11:36 (UTC)

Email : charliechaplin.dev@gmail.com
Google ID : 117833363030761934622

Hangouts Bot : No

[+] Activated Google services :
- Hangouts

[+] YouTube channel (confidence => 50.0%) :
- [Charlie Chaplin] https://youtube.com/channel/UCe7sQfrqTHc-hWXdenf7VxQ

Google Maps : https://www.google.com/maps/contrib/117833363030761934622/reviews
[-] No reviews

Google Calendar : https://calendar.google.com/calendar/u/0/embed?src=charliechaplin.dev@gmail.com
[-] No public Google Calendar.
```

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 Iris-Sec that we've linked to above cracked open the whole case!

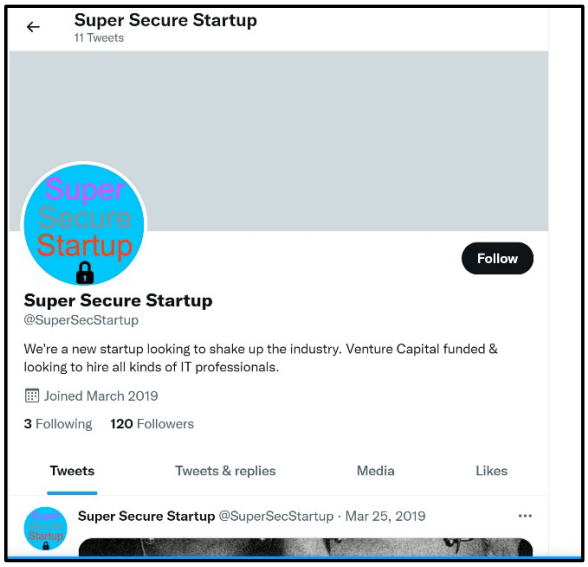
APPENDIX C
CTF WRITEUP: HTB: WE HAVE A LEAK

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 corner of 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 that is given is "Super Secure Startup's private information is being leaked; can you find out how?" I began with a simple Google search of Super Secure Startup. The first result shows us a Twitter page: https://twitter.com/supersecstartup?lang=en

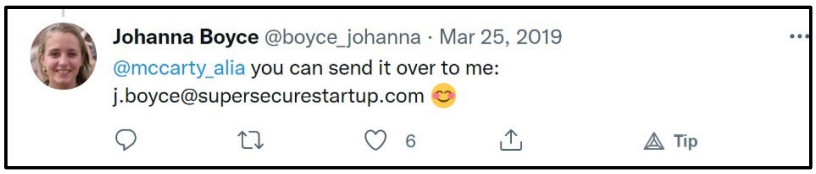


This page pretty clearly looks like something for a capture the flag challenge, so I knew I was onthe right track. I began clicking on everything and anything I could on the site, looking through photos, comments, and even people who liked the posts. A post that stood out to me was the following:

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

Josh Terranwald is a web developer who seems to like YouTube and dogs. There is not much here, but I put his profile on the back burner 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 plans from 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.

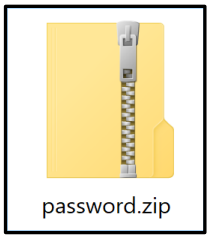
https://twitter.com/BiankaPhelps

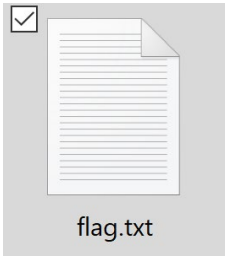
Bianka is an HR professional at Super Secure Startup. Again, she seemed to post some sensitive information about the company, including what seems to be an SSH default password onone of their whiteboards. This may be helpful in the future.

Returning to the initial password-protected zip file I downloaded, the first password was given to us by Hack the Box. 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, Johanna Boyce, 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 an SSH default password in 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 our flag.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 as super 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 to open the zip folder before I started searching. I totally forgot that it was a part of the challenge, so I spent quite a 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 to find the next piece of information, you are probably following a red herring, which is something

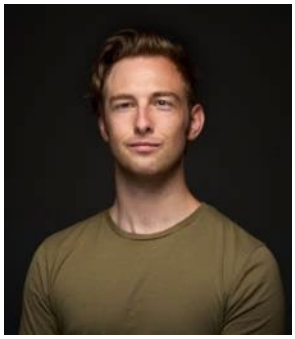
to be aware of. If you find yourself searching for extended periods of time, take a break and re-evaluate what information you have and what you can use.

AUTHORS

Albert Tay, an IT & Cybersecurity faculty member at Brigham Young University, received his Ph.D. in Communication and Information Sciences from the University of Hawaii, Manoa. Dr. Tay is co-PI on the NSF CyberCorps Scholarship for Service grant ($3.7 million).

Prior to joining BYU, Dr. Tay managed Utah's Statewide Longitudinal Data Systems program and served as the project director for the IES FY 2015 SLDS grant ($6.7 million). Dr. Tay has also taught IT courses at various universities and managed IT departments and projects in various industries.

Sebastian Hayes is currently a cybersecurity student at Brigham Young University. Sebastian is a teaching assistant for IT & Cybersecurity courses. He also serves as a research assistant at the Cybersecurity Research Laboratory. He is president of the Network Engineering Student Association and program director for Kids Who Code. He participated in NCAE CyberGames (placed 1st in regionals 2022 and 2023) and National Cyber League CTF (placed 3rd in Fall 2023). He has also assisted in creating the BYU public CTF (2022, 2023), BYU STEM Camp CTF (2023), and BYU Cybersecurity Camp CTF (2022, 2023).



Drew Wilson is a Computer Science student at Brigham Young University. Drew is a teaching assistant for Computer Science courses. He also serves as a research assistant at the Cybersecurity Research Laboratory. He is vice president of the Cybersecurity Student Association and is interested in applying machine learning to cybersecurity tools and processes. He has participated in many cybersecurity competitions, including the National Cyber League, where his team placed 3rd, and Hack the Building, which emphasized securing ICS technology against APTs.

Emmie Hall is currently a cybersecurity student at Brigham Young. Emmie works in the Office of Information Technology. She was a teaching assistant for an IT & Cybersecurity course. She also serves as a research assistant at the Cybersecurity Research Laboratory. She participated in NCAE CyberGames (placed 1st in regionals 2023).

Dallin Kaufman is currently a cybersecurity student at Brigham Young. He volunteers at the Cybersecurity Research Laboratory. He also teaches introductory cybersecurity classes and leads the CTF group for the Cybersecurity Student Association. He participated in the National Cyber League Team competition (placed 3rd nationally) and the National Collegiate Cyber Defense Competition (placed 8th nationally).