Journal of Information Systems Education

Volume 37
Issue 1
Winter 2026

Creating a Persistent Competition to Prepare Undergraduate Cybersecurity Students for National Cyber League Competitions

Brandon P. Grech

Recommended Citation: Grech, B. P. (2026). Creating a Persistent Competition to Prepare Undergraduate Cybersecurity Students for National Cyber League Competitions. *Journal of Information Systems Education*, 37(1), 98-132. https://doi.org/10.62273/GKDZ1277

Article Link: https://jise.org/Volume37/n1/JISE2026v37n1pp98-132.html

Received: March 10, 2025
First Decision: July 3, 2025
Accepted: August 22, 2025
Published: March 15, 2026

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 37(1), 98-132, Winter 2026
https://doi.org/10.62273/GKDZ1277

Creating a Persistent Competition to Prepare Undergraduate Cybersecurity Students for National Cyber League Competitions

Brandon P. Grech
Center for Cybersecurity
Anderson University
Anderson, SC 29621, USA
bgrech@andersonuniversity.edu

ABSTRACT

The demand for cybersecurity professionals continues to be a pressing need for the global workforce. Institutions of higher learning have been launching new cybersecurity programs to help meet this demand. This research describes how an undergraduate cybersecurity program that launched in the Fall of 2020 used free and open-source software, cloud computing, and a domain name registrar to create a persistent cybersecurity competition for the students with high impact in National Cyber League rankings at a low financial cost. This competition has been available both on-campus and off-campus for students to access, compete, and ultimately prepare themselves for national cybersecurity competitions, such as the National Cyber League. This solution has served 182 students with 456 challenges across several categories such as: Network Analysis, Web, Open Source Intelligence, Log Analysis, Digital Forensics and Incident Response, Cryptography, Password Cracking, Current & Past, and Miscellaneous. Over the past five years, this solution has allowed for challenges to be solved 11,633 times in 32,141 attempts by the students and has been identified as an important resource in preparing students to place as high as fifth in the United States of America (out of 500+ colleges and universities) in the National Cyber League. This research will highlight platform details and will also share student feedback about how this persistent cybersecurity competition prepared students to perform against students from other institutions.

Keywords: Cybersecurity, Competition, Gamification, Student satisfaction, Open source

1. INTRODUCTION

Over the last decade, there has been a surge of cybersecurity undergraduate program offerings. As of 2023, there are 377 United States institutions that offer cybersecurity programs that meet the NSA's CAE-C criteria for academic rigor (Crabb et al., 2024). Some of these programs are starting from scratch while others are being built by existing departments that specialize in related fields. For example, building a cybersecurity degree program with limited resources has been researched and conducted by leveraging existing faculty that teach computer science or related fields at institutions (Bell & Oudshoorn, 2018).

This research is aimed towards either new or existing faculty tasked with creating and leading cybersecurity programs that may have limited funds. Research has shown that cybersecurity competitions are an effective way in educating students (Cheung et al., 2011). This research shows how faculty can help prepare students for cybersecurity competitions and the workforce with a low-cost training platform.

As cybersecurity students and professionals continue to develop and master their craft, they may participate in various cybersecurity competitions to hone their technical skills and improve their ability to solve problems (Wee et al., 2016). Capture-the-Flag (CTF) competitions allow either individuals or teams to compete within certain cybersecurity-related challenges and earn points by finding a "flag" or performing a task. There are four styles of CTFs: Jeopardy, King of the Hill (KotH), Attack & Defense, and Linear CTF (CTF.zone, n.d.).

A Jeopardy CTF, similar to the television show, allows competitors to select any unsolved challenge and attempt to solve it to earn points. The points available typically range depending on the difficulty of the challenge. A Jeopardy CTF commonly has multiple categories with multiple challenges within each category. Some common categories of challenges include Reconnaissance, Open Source Intelligence (OSINT), Cryptography, Password Cracking, Web, Web Application Exploitation, Digital Forensics, Network Traffic Analysis, Log Analysis, Exploitation, and Reverse Engineering (CTF.zone, n.d.; National Cyber League, n.d.; Raymond, 2019). The categories listed have clear overlaps and a CTF competition may not have each of these categories. For example, password cracking could be a category of its own, be a subset of cryptography, or be integrated within other categories (e.g., a challenge where a password hash is sent over the network and must be extracted could be listed as a network traffic analysis challenge).

A King of the Hill (KotH) competition allows competitors to attack one or more live servers to earn points. After successfully gaining access to a server, competitors attempt to secure the system to avoid other competitors earning credit for successfully exploiting the same server. In a KotH competition, all teams attack the same one or more servers. One of the strengths of KotH competitions is the ability to teach offensive penetration testing skills as well as finding and mitigating vulnerabilities (Bock et al., 2018).

An Attack & Defense competition consists of each competitor (individual or team) having their own server that requires defending from other teams while the competitor attacks the servers owned by other competitors. In an Attack & Defense competition, competitors defend their own server while attacking others. This differs from a KotH competition where in a KotH competition different competitors attack and eventually defend the same server. In other words, only one "king" controls the server at a time.

Lastly, a Linear CTF is a category of CTFs where competitors must solve multiple challenges in succession to receive the "flag."

1.1 Goals of This Paper

By analyzing the usage of a persistent CTF platform, this research looks to gain a better understanding of how students have interacted with the platform outside of a classroom setting. This platform is regularly used as an extracurricular platform during live in-person weekly practices. The majority of time students access this platform is outside of classes and practices as students spend hours attempting to solve challenges. This research attempts to retrace, replicate, and share the installation steps of this CTF platform while also sharing examples of CTF challenges and potential solutions to challenges within each CTF category. This research is also exploring the opinions of high-performing competition students regarding the platform and how they believe it may have prepared them for the National Cyber League. Specifically, the research questions are as follows:

- What are the financial costs and technical steps required to deploy a persistent Capture-the-Flag (CTF) platform?
- How has a persistent Capture-the-Flag (CTF) platform been used by undergraduate cybersecurity students?
- What are the top-performing students' perspectives on the persistent Capture-the-Flag's effectiveness in preparing for cybersecurity competitions, such as the National Cyber League?

This paper will begin by addressing the first question by sharing financial costs and technical steps regarding how to deploy a persistent Capture-the-Flag platform. This paper will also share some examples of CTF questions for each category. The second question will explore the usage statistics regarding the total number of challenges, solve count, score distribution, solve percentages per challenge, submission percentages (solves vs fails), and a category breakdown. The third question will query students that have

participated in both this persistent CTF and the National Cyber League (NCL) about their opinion regarding the persistent CTF's effectiveness in preparing the students for the NCL competitions.

1.2 Contributions of This Paper

The number of CTF competitions has been growing over the past decade. For example, CTFtime's archives show 274 CTF events were hosted in 2022, 333 CTF events in 2023, and 350 CTF events in 2024 (CTFtime, 2022, 2023, 2024). These CTF competitions are typically only available for only one to three days. This paper explores how CTF competitions can be used in a persistent manner (the CTF never ends/expires) and grow over time to help develop students outside of class. This paper aims to showcase to cybersecurity faculty how a CTF can be created and used to prepare students for cybersecurity competitions. Answering the previously-stated research questions will hopefully be valuable to help other cybersecurity faculty members forge their own path in creating persistent CTF platforms and prepare their students for competitions, such as the NCL.

This research is focused on preparing students for the National Cyber League as the National Cyber League has been found to be well mapped to cybersecurity courses and learning outcomes while also students enjoy the NCL experience (Wang & D'Cruze, 2022). Prior National Cyber League competitors that are now currently employed have shared that their NCL experiences improved competence and confidence to help prepare their skills for the workforce (Zeichick, 2024).

Thomas et al. (2019) found that lack of knowledge leads to being less motivated in competition as well as training prior to the competition benefits the engagement of the student during competition. This research paper shows how a low-cost solution can be used to give students more knowledge and preparation prior to a competition, such as the National Cyber League.

1.3 Structure of This Paper

Section 2 assists with explaining critical terms used within this paper regarding cybersecurity and CTF competitions. Section 3 explores prior work related to CTF competitions. Section 4 describes the required infrastructure to support the persistent CTF platform and showcases the specific steps needed to install CTF software application in a secure manner with HTTPS support. Section 5 showcases each category of challenges with example challenges and solutions. Section 6 presents the usage statistics of the CTF platform. Section 7 explores the survey results of the students regarding their opinions of the CTF platform. Section 8 concludes the research and contributions.

2. BACKGROUND AND TERMINOLOGY

This section defines critical terms used within this paper regarding cybersecurity and CTF competition.

2.1 Capture-the-Flag

Within cybersecurity, the term *Capture-the-Flag (CTF)* refers to a competition where a player or team of players attempts to solve cybersecurity-related challenges and retrieve a flag. This flag is then submitted as proof that the challenge was completed successfully. Points are awarded to the player or team for their successful endeavor. This concept stems from the traditional outdoor game (also called "Capture-the-Flag") where two teams attempt to find the other team's physical flag, retrieve it, and bring it back safely for points or victory. Throughout this research paper, the term Capture-the-Flag (CTF) will only reference the cybersecurity competition. One of the most popular resources for CTF competitions is CTFtime as CTFtime tracks and aggregates global CTF events (Davis et al., 2014). CTFtime is a popular website that serves as a centralized location of past, current, and upcoming CTF events across the world (CTFtime, n.d.). CTFtime also provides a leaderboard ranking of CTF teams each year and allows teams to author writeups (solutions to past CTF challenges).

2.2 CTF Challenge Flag

Within CTF challenges, the term *flag* refers to a piece of evidence proving an individual or team successfully completed a challenge. This flag is typically a string of characters. This string may either be a word, series of words, or a random string of characters. The competitors may either submit the flag as it is or may need to wrap the flag within certain symbols ({flag}, [flag], (flag), etc.). Some other forms of flags are files or simply an answer to a question (similar to a question/answer response). Competitors must understand what a flag looks like when solving a CTF challenge and how to submit it correctly on the platform to earn points. Competitions, such as the NCL, use accuracy (percentage of submitted flags were correct) as a tiebreaker, thus increasing the importance of understanding how to submit the flag to avoid being penalized for an incorrect submission.

2.3 National Cyber League

The National Cyber League (NCL) is a Jeopardy-style CTF that is available during the Spring and Fall semester every year to students enrolled in a U.S. collegiate institution. The majority of the NCL players are college students; however, high school students are also eligible to compete in the NCL. During each season (Spring and Fall), the NCL has an Individual Game and a Team Game. The Individual Game spans three days (Friday through Sunday) and the Team Game typically follows a couple of weeks later and spans three days (Friday through Sunday). Students work on their own for the Individual Game and can have a team of from one to seven students for the Team Game. Both the Individual Game and Team Game consist of challenges across nine modules (National Cyber League, 2024):

1. Open Source Intelligence: Use publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.
2. Cryptography: Identify techniques used to encrypt or obfuscate messages and leverage tools to extract plain text.
3. Password Cracking: Identify types of password hashes and apply various techniques to efficiently determine plain text passwords.
4. Log Analysis: Use the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.
5. Network Traffic Analysis: Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.
6. Forensics: Use the proper tools and techniques to analyze, process, recover, and/or investigate digital evidence in a computer-related incident.
7. Scanning & Reconnaissance: Identify and use the proper tools to gain intelligence about a target including its services and potential vulnerabilities.
8. Web Application Exploitation: Identify actionable exploits and vulnerabilities and use them to bypass the security measures in online services.
9. Enumeration & Exploitation: Identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.

3. RELATED WORK

This section highlights related publications and how this research differs from each of them.

3.1 Cybersecurity Knowledge and Skills Within CTF Challenges

Švábenský et al. (2021) analyzed nearly 16,000 writeups of CTF challenges between 2012 and 2020. This analysis attempted to understand the CTF challenge topics and how they relate to current Cybersecurity Curricular Guidelines (CSEC2017) Knowledge Areas. The CSEC2017 Knowledge Areas are Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, and Societal Security. This research showed how cryptography and network security are the most prominent topics within CTF challenges. Furthermore, this work shared that CTF challenges allow competitors to learn and practice technical skills; however, they lack the "people" aspect

in cybersecurity, and designing CTFs to address this could lead to reaching a broader, non-technical audience and influence more prospective students and adults into the cybersecurity workforce. Each of these CTF challenges came from competitions that have ended and are no longer available to interact with. Švábenský et al.'s (2021) research dealt with temporary, non-persistent CTF competitions while this research is exploring a persistent CTF competition.

3.2 Comparing Open Source CTF Platforms as Cybersecurity e-Learning Tools

Karagiannis et al. (2020) compared the following open source CTF platforms: Facebook CTF (FBCTF), CTFd, Mellivora, and Root the Box with the following evaluation criteria: functionality, extensibility, teaching presence, flag and challenge management/submission, social presence, sustainability, portability, and various attributes presented to participants via one-on-one interviews. The research discovered that CTFd made it easier for beginners to understand the challenges clearly and engage with the challenges in a quick manner. The research also noted that CTFd supports dependencies being built into the challenges (linear or by condition) while also having a better scoreboard, set of graphs, and team-based statistics. Lastly, the findings described CTFd's deployment and installation process as easy and fast. These features make CTFd an effective option from an educational perspective for beginner students and facilitators.

3.3 Using CTF Tournaments in Higher Education

Gonzalez et al. (2019) conducted a CTF tournament to reinforce the topics learned in a cybersecurity course. This research used Mellivora as the open source CTF platform for the CTF tournament. The CTF tournament was conducted over two days in which 27 students spent over 20 hours attempting to complete 22 challenges. These challenges spanned across the categories of firmware, forensics, MITM (man-in-the-middle), network forensics, networking programming, programming, reversing, and web. The students played a unique factor in the development of the challenges as they researched the news, proposed one or two cybersecurity topics, and voted on which topics would be covered in the class and CTF tournament. This CTF tournament example is a unique, but effective, method of using CTFs in the classroom. Similar to Švábenský et al.'s (2021) research, Gonzalez et al.'s (2019) CTF tournament research also dealt with a temporary, non-persistent CTF competition while this research is exploring a persistent CTF competition.

4. SUPPORTING INFRASTRUCTURE AND INSTALLATION

The technical infrastructure that supports this persistent Capture-the-Flag platform includes three components: domain name registrar, cloud hosting provider, and the Capture-the-Flag framework software.

4.1 Domain Name Registrar

A domain name registrar is a business that manages domain names and the IP addresses assigned to them, and works between the party registering a domain name and the appropriate Regional Internet Registries (Hoffman & Fujiwara, 2024). A domain name registrar allows users to purchase domain names and use them for websites or other purposes. In this deployment, Namecheap was the registrar used as it offered low-cost deals (Namecheap, n.d.). Initially, the domain *teameffort.work* was purchased for $2.17 a year that included the cost to register teameffort.work ($1.99) plus a $0.18 ICANN fee. After the promotional period (two years) expired, the domain's cost increased to $11.16 a year (less than $1 a month).

Once a domain is purchased, the customer can edit the DNS settings and add an A Record to point to a specific IP address. In the following example the subdomain of ctf (ctf.teameffort.work) will resolve to 66.228.56.112. The IPv4 address of 66.228.56.112 is the address of the server that is hosting the CTFd platform. Additional A Records can be added to Namecheap to resolve additional hosts. For example, Figures 1 and 2 show how a user can add an IP address for the root domain (teameffort.work) or point a different subdomain to a different IP address.

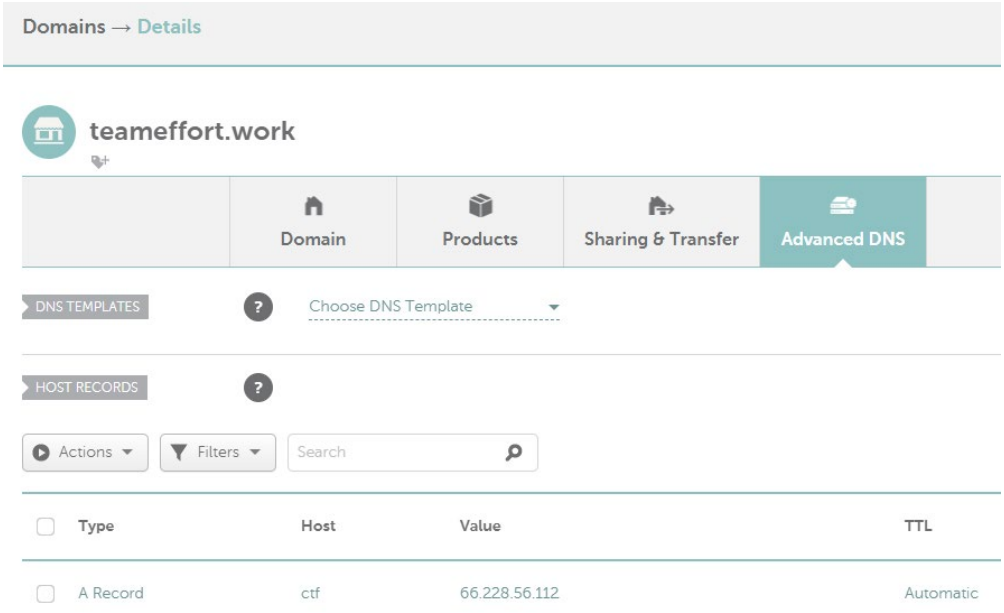


Figure 1. Namecheap DNS Settings Example - 1

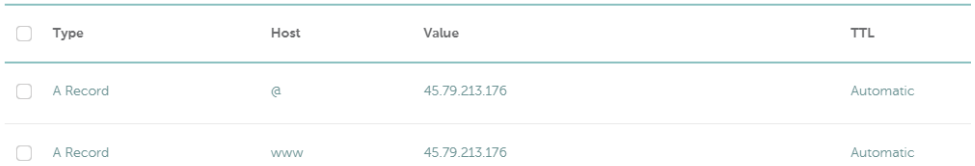


Figure 2. Namecheap DNS Settings Example - 2

4.2 Cloud Hosting Provider

A cloud hosting provider is a business that provides information technology resources that are accessible via the Internet. A cloud hosting provider allows customers to have access to computing resources that may be located at various data centers throughout the world. This solution currently leases an Ubuntu 24.04 LTS server with 1 CPU Core, 2 GB RAM, and 50 GB Storage for $12 a month from the company Linode. Linode offers various plans to use shared virtual machines with balanced power and performance (Linode, n.d.). Linode was acquired by Akamai Technologies in 2022 and the monthly cost for most plans increased by 20%. This implementation also has backups enabled at a current cost of $2.50 a month.

Figure 3 shows the Linode account with an active Ubuntu 24.04 (labeled “ctf”) on the Linode 2 GB Plan with an IPv4 address of 66.228.56.112 located in a different state from that where the institution is physically located.

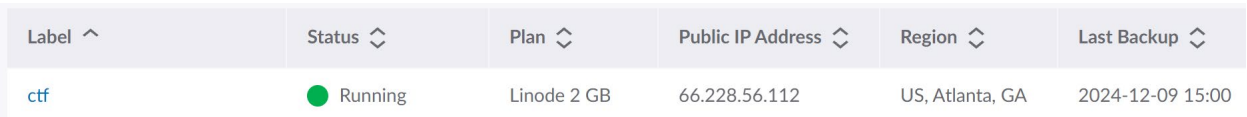


Figure 3. Ubuntu 24.04 LTS Server on Linode - 1

Figure 4 shows the Ubuntu 24.04 LTS server with 1 CPU Core, 2 GB RAM, and 50 GB Storage that is used to host the CTF framework software.

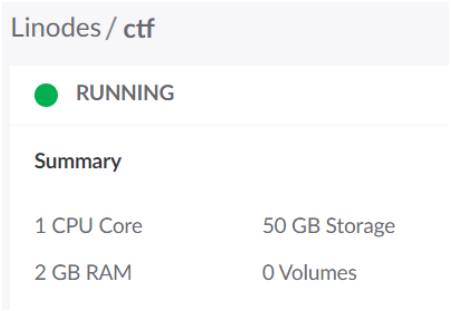


Figure 4. Ubuntu 24.04 LTS Server on Linode - 2

4.3 Capture-the-Flag Framework Software

Capture-the-Flag framework software creates the entire gaming experience for the competitors. This typically includes (at minimum) a web interface, scoring/grading capabilities, and a scoreboard. Other features may include maps, themes, embedded media, file server, email, and challenge assessment statistics (Karagiannis et al., 2020). CTFd was the Capture-the-Flag framework of choice as it is free, open source, and provided more desired features than other CTF Frameworks (such as Facebook CTF) according to Karagiannis et al.'s (2020) research.

4.4 Installation

The steps to install CTFd as a Docker instance with HTTPS include ensuring the requirements are met, purchasing a domain name, administratively accessing an Ubuntu machine with a public IP address, ensuring the domain name resolves, completing the CTFd Docker installation, retrieving an HTTPS certificate, configuring the webserver to use the appropriate certificate for HTTPS, and starting the CTFd instance. These technical steps can be seen in Appendix A. In this solution, Let's Encrypt was used as the Certificate Authority as it is a free, automated, and open certification authority (Let's Encrypt, n.d.). The webserver software nginx was used as it is the default for the CTFd Docker installation.

5. CHALLENGES

Capture-the-Flag competitions that use the Jeopardy format typically contain various categories. This platform uses ten separate categories: Open Source Intelligence (OSINT), Current & Past, Password Cracking, Crypto, Network Analysis, Log Analysis, Digital Forensics and Incident Response (DFIR), Web, Miscellaneous, and NCL Archive. The categories are loosely derived from the National Cyber League modules, as stated previously. Now we will examine each category and provide an example challenge within each category along with a possible means to solve the challenge.

5.1 Open Source Intelligence (OSINT)

Open Source Intelligence (OSINT) is any intelligence produced from publicly available information that is collected, exploited, and disseminated (Public Law 109-163, 2006). The OSINT category is intentionally the first category for the competitors. The reason for OSINT being the first category is that no special software is required to begin solving these tasks. Competitors typically are already comfortable with sleuthing the Internet and using various search platforms to find publicly available information (e.g., search engines, social media, reverse image search, publications). This allows students to not feel discouraged by a frustrating installation process of specific tools and technologies. Instead, students gather some quick

challenge solutions and see their name on the scoreboard. Currently, this persistent CTF platform has 97 OSINT challenges.

For example, nine "Security" question challenges were created to demonstrate to the students how insecure security questions are (if answered correctly by the user) and how easily the answers to these questions can be found. This also allows students to get to know their cybersecurity competition coach (one of their faculty members) via OSINT methods. For example, "Security" question #1 asks the competitors to find the CTF creator's middle name.

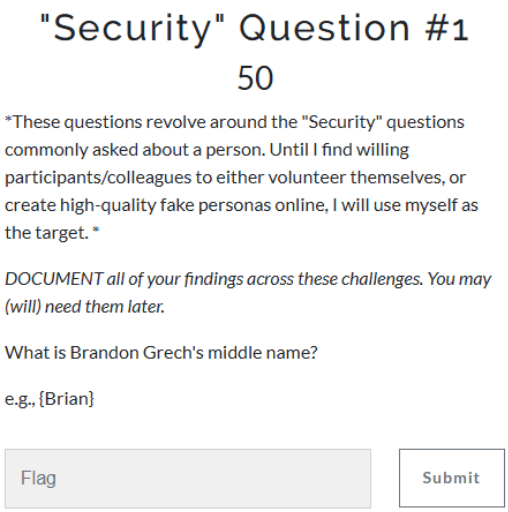


Figure 5. OSINT Challenge Example

A 50-point value is relatively low compared to other challenges on this persistent CTF; therefore, the difficulty should be relatively low. Students typically solve this challenge by using a search engine to search for the person's name and may notice the middle name located in the associated LinkedIn profile for this person.

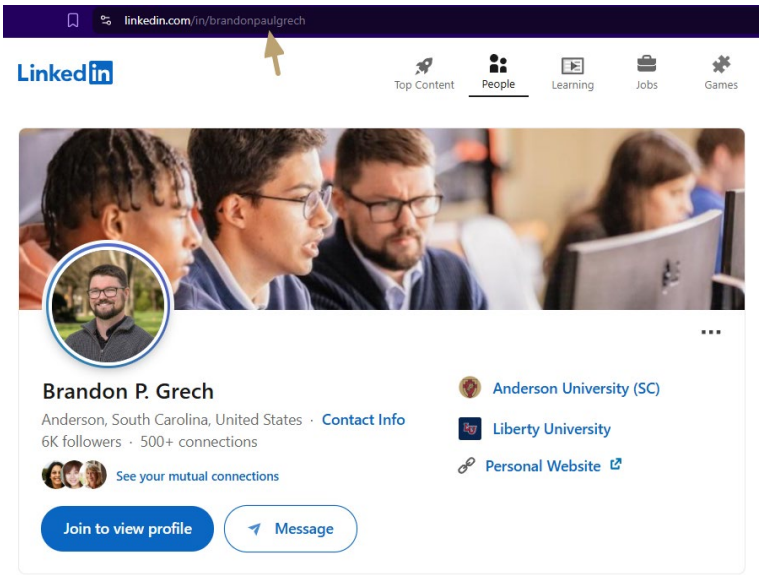


Figure 6. OSINT Challenge Solution Example

Some other OSINT challenges include: "whois" lookups, reverse image searches, archived web pages, media EXIF/metadata, satellite imagery, GEOINT based on images/videos, satellites, Twitter/X, and others.

5.2 Current & Past

This section is an uncommon category for CTFs; however, this platform uses it to have students dive into cybersecurity-specific topics that are either current or have some historical significance. At this time, this persistent CTF platform has 15 Current & Past challenges.

For example, within the Current & Past section, one challenge shows students an old photograph. Students must figure out that the person in Figure 7 is Grace Hopper. Hopper worked on the Mark I, an early prototype of the electronic computer (Norwood, 2017).

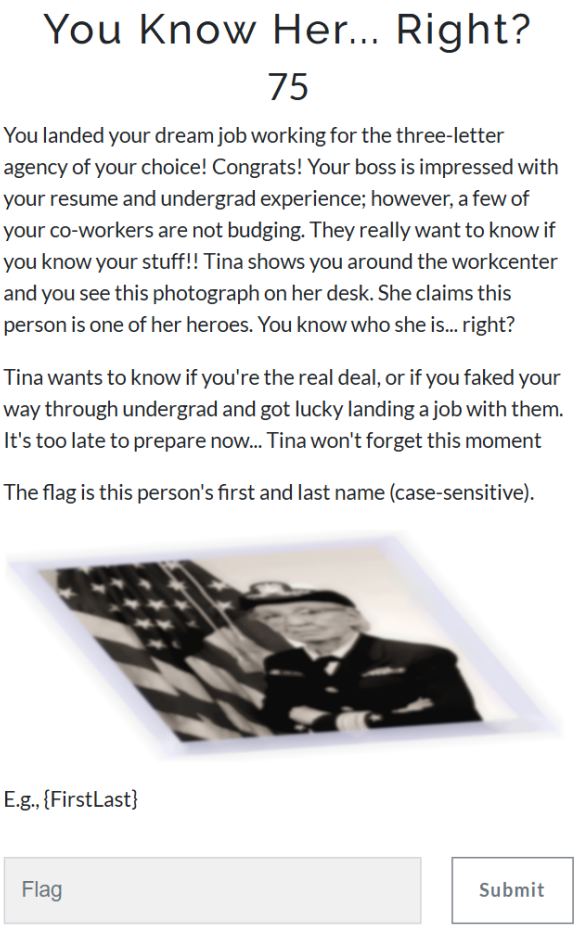


Figure 7. Current & Past Challenge Example

Students typically solve this challenge by either modifying the image back to an upright position and performing a reverse image search using the modified image or by performing a search engine query looking for female cybersecurity heroes in history. TinEye and Google Images both offer reverse image searches (Google Images, n.d.; TinEye, n.d.). During the creation of this challenge, they were only able to identify the photo as Grace Hopper if the student corrected the orientation of the photo (shown in Figures 8 through 10); however, advancements in Google Images have now allowed this challenge to be solved by a simple reverse search on Google Images (shown in Figure 11).

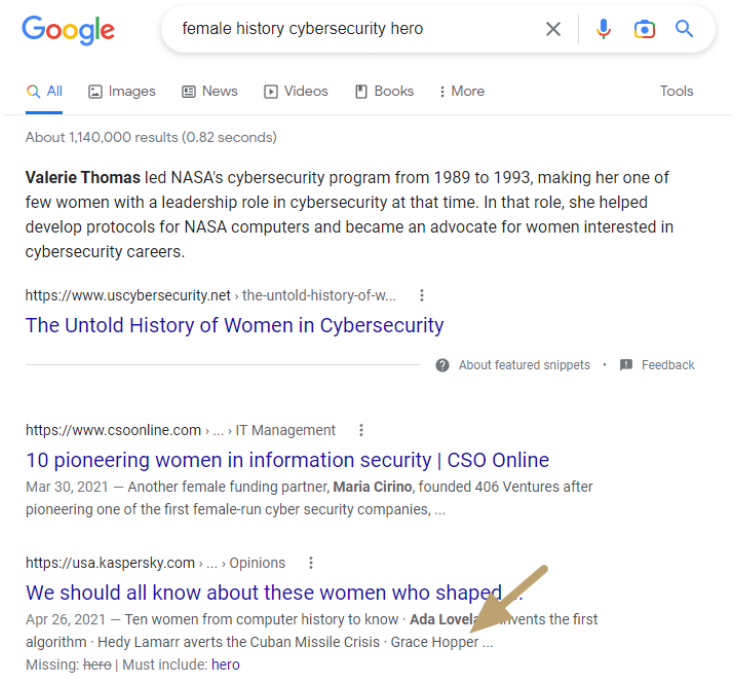


Figure 8. Current & Past Challenge Solution Example - 1

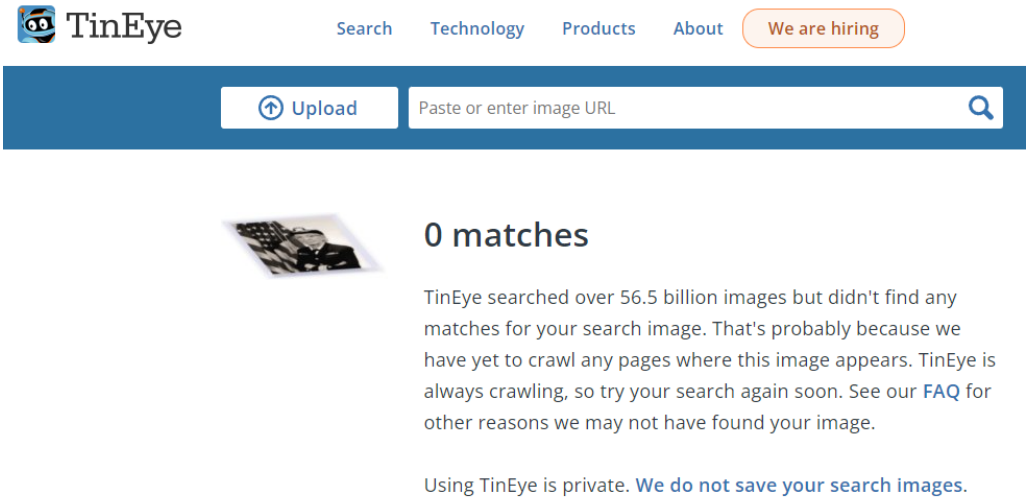


Figure 9. Current & Past Challenge Solution Example - 2

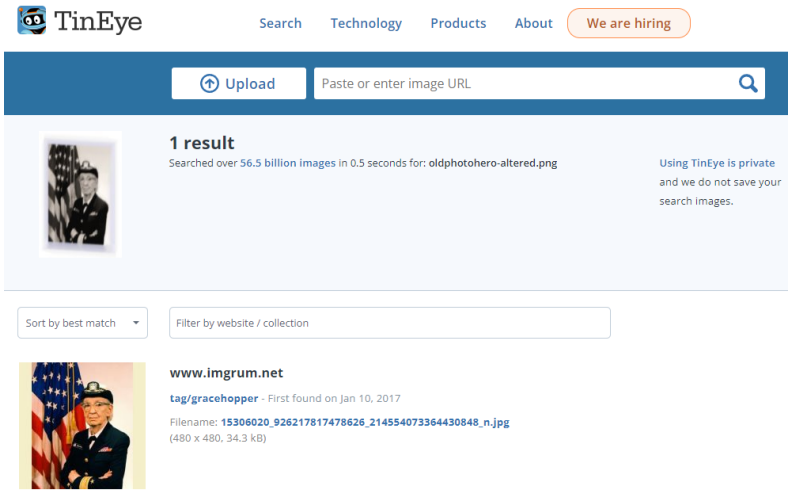


Figure 10. Current & Past Challenge Solution Example - 3

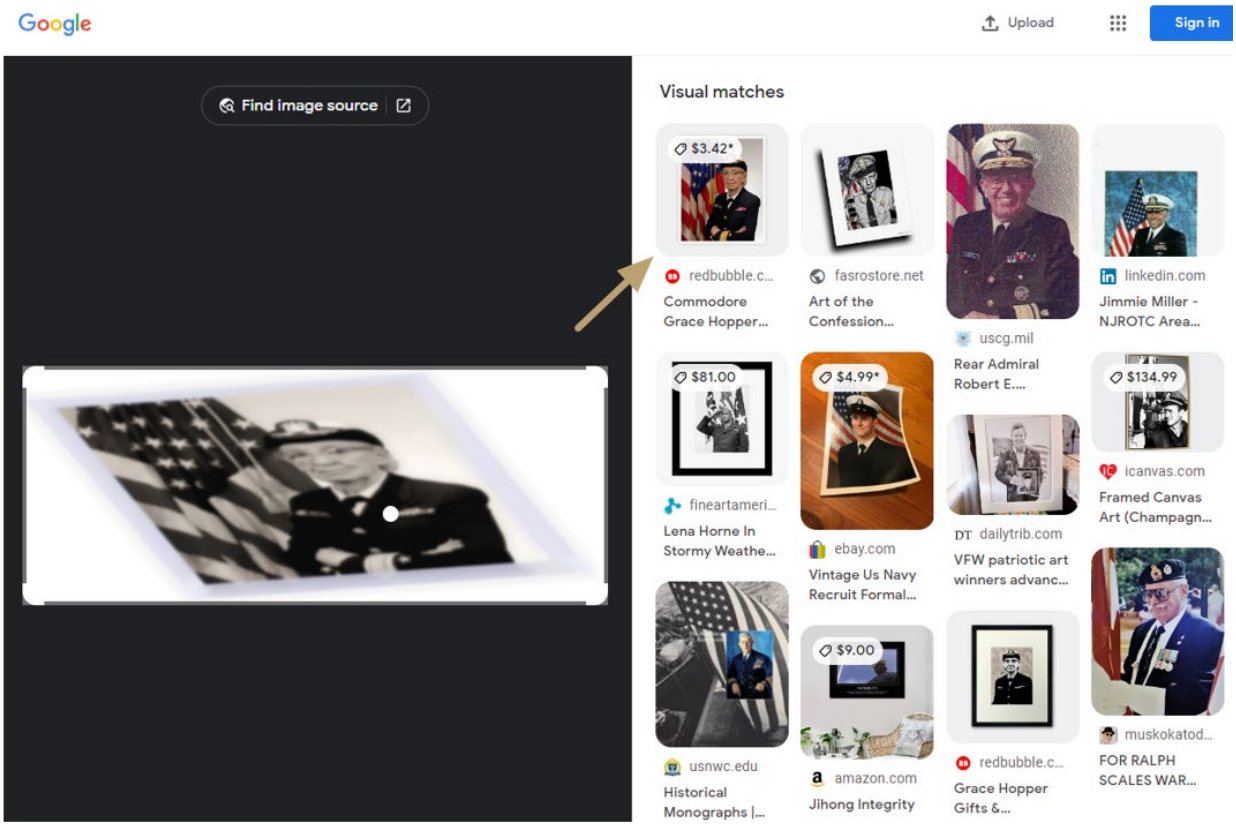


Figure 11. Current & Past Challenge Solution Example - 4

Some other "Current & Past" challenges include identifying cybersecurity companies based on a partial logo, various questions about historic malware, and questions about recent cybersecurity news.

5.3 Password Cracking

This category contains challenges to crack a password hash. A password hash is the result of a one-way encryption function (Temoshok et al., 2025). These challenges typically consist of giving students a hash and directions on what to use to crack them. These directions may include a wordlist, adding numbers to the words, or other mangling techniques. Currently, this persistent CTF platform has 113 Password Cracking challenges.

For example, nine "SHArkba1t! Ooh ha ha! #[1–9]" challenges were created. Each of these challenges contains a different unsalted SHA1 password hash to crack. (Unsalted means that no extra random data (a salt) was added before hashing.) In the SHArkba1t! Ooh ha ha! #5 challenge (Figure 12), the students have already been given a clean (no profanity) wordlist to use to crack this hash.

Figure 12. Password Cracking Challenge Example

Students can use a tool such as John the Ripper to crack this hash with a command such as "john --wordlist=<wordlist.txt> --format=raw-sha1 <filecontainginghash>." Some other Password Cracking challenges include: MD5 hashes, SHA256 hashes, SHA512 hashes, yescrypt hashes, and various hashes that require mangling and/or custom wordlist generation. Challenges that contain more complex password cracking challenges are found in the Crypto section.

5.4 Crypto

This category contains challenges that are cryptography-related. This includes various encoding and encrypting techniques. This section also includes password cracking. However, different actions must occur for the password cracking to be successful (e.g., *2john programs, mangling, custom wordlists). In other words, the password cracking challenges within the crypto section require more than simply a one-line command to crack the password hash. Currently, this persistent CTF platform has 73 crypto challenges.

For example, one of the easier crypto challenges is called "Numbers." The "Numbers" challenge (Figure 13) gives the students an image of various numbers between curly braces. Curly braces are required for all flag submissions in this CTF; however, the format of flag submissions will vary across different CTFs. The challenge asks students to convert the numbers to a string. Students must determine that this challenge uses A1Z26. A1Z26 is also referenced as Letter-to-Number, Number-to-Letter, or numbered alphabet (Boxentriq, n.d.; Cryptii, n.d.; CyberChef, n.d.; dCode.xyz, n.d.; PlanetCalc, n.d.). Regardless, in this code, each letter of the alphabet is referenced by its position within the English alphabet. Since A is the first letter of the alphabet A=1. Since B is the second letter of the alphabet B=2. This pattern continues (C=3, D=4, E=5, and so on). This continues through Z where Z=26.

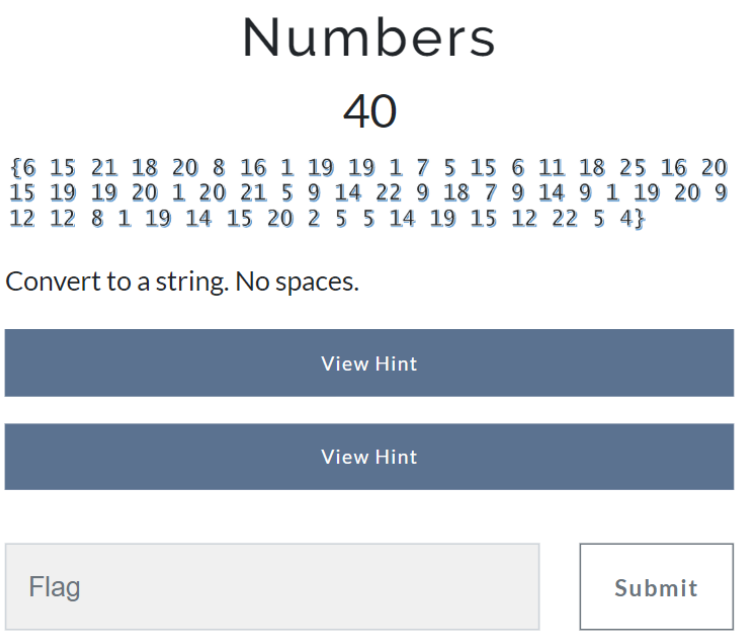


Figure 13. Crypto Challenge Example

This challenge has two hints. CTFd offers the ability to have a hint cost the student a set value of points for each hint; however, this persistent environment allows all hints to be utilized without penalty. Mark Rober, a well-known YouTuber and former NASA and Apple engineer, gave a talk at TEDxPenn in 2018 showcasing that people attempt more and therefore learn more when teachers do not subtract points for failed attempts (Rober, 2018). This persistent platform uses this same approach by not penalizing students for using hints or several attempts on a question. Only a select few of this persistent CTF's questions have a submission limit (to discourage brute-force attempts); however, those are the exceptions. Students have also been made aware of various Cryptography articles that reference common cryptography encoding and encrypting methods. Some common websites students use to gain familiarity with these encryption methods and ultimately decipher and solve these challenges include dCode, Boxentriq, and Charity Barker's blog titled charcharbinks (Barker, 2020; Boxentriq, n.d.; dCode.xyz, n.d.). Some other Cryptography challenges include: various encoding schemes (e.g., binary, octal, hexadecimal, base32, base64), historical ciphers, symbol ciphers, cryptocurrency tracking, digital certificates, and more complex password cracking tasks (leaked passwords, encrypted files, and custom wordlists scraped from online resources).

5.5 Network Analysis

This category contains challenges that require network-related questions or network traffic analysis. This includes packet capture (pcap) analysis, network vulnerability research (CVE and CVSS), URL, MAC, and IP address questions, wireless network mapping, connecting to various live servers (via netcat, SSH, FTP, etc.), and extracting data (credentials, HTML pages, strings, and steganography) out of packet captures using various encoding and encrypting techniques. Currently, this persistent CTF platform has 43 network analysis challenges.

For example, nine challenges titled "Starter PCAP #[1–9]" were created. Each challenge contains the same packet capture (pcap). This packet capture is relatively small and only contains ~7,000 packets. This pcap and set of questions are designed to be a relatively easy set of questions to get students familiar with the basics of Wireshark and packet analysis. An external WordPress website is to host this pcap; however, this pcap could have been uploaded to the CTFd application for a direct download. Starter PCAP #3

challenges the students to discover the IP address for the dev network interface card (NIC) that has MAC address of 00:0c:29:eb:f0:4d.

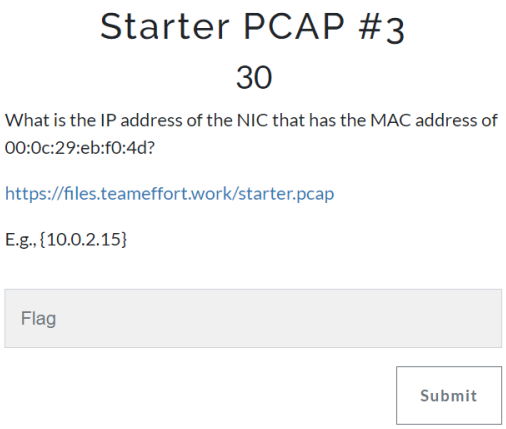


Figure 14. Network Analysis Challenge Example

Students may choose to analyze the packet capture in Wireshark and notice the very first packet within this packet capture contains the MAC address the challenge asks about (00:0c:29:eb:f0:4d) and the source (src) IP address associated with that device (172.29.33.47).

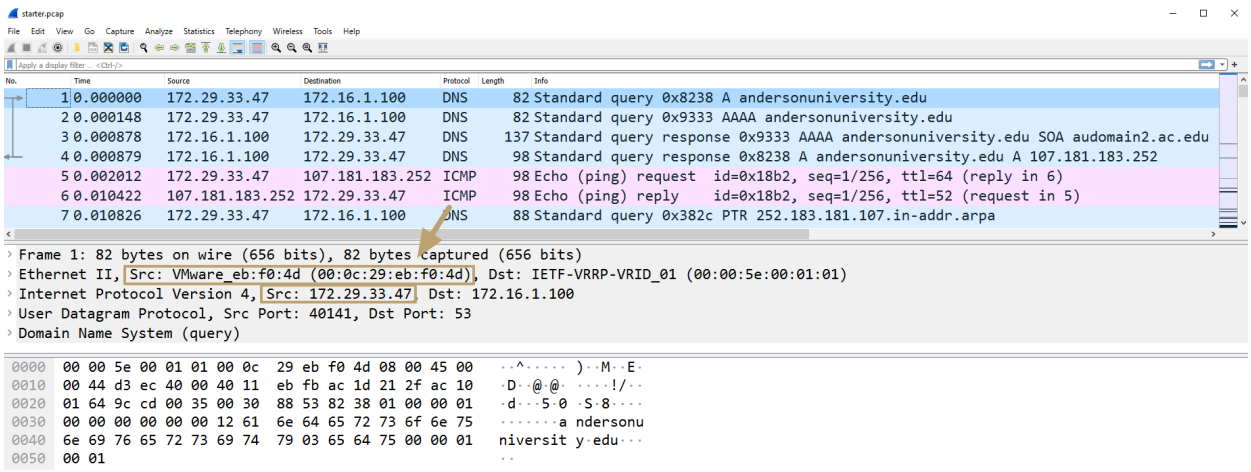


Figure 15. Network Analysis Challenge Solution Example

5.6 Log Analysis

This category contains challenges that require some tasks related to analyzing logs. Students investigate log files and answer questions about the data these logs indicate. These challenges include wordlists, sudo usage, ssh access attempts, and command history. Currently, this persistent CTF platform has 13 log analysis challenges.

For example, a challenge titled "sudo again" was created where students must search through a Linux's auth.log file to identify when a user logged in to the machine and executed elevated commands with sudo. This challenge is an example of how CTFd can be used to reward students as long as one of multiple possible flags is submitted.

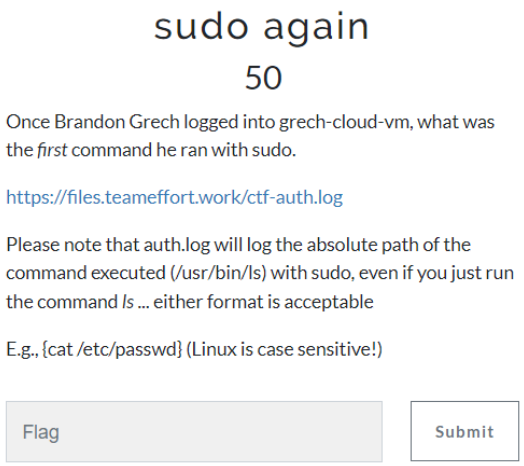


Figure 16. Log Analysis Challenge Example

5.7 Digital Forensics and Incident Response (DFIR)

This category contains challenges that require some type of digital forensics or incident response analysis. This includes data extraction/carving, EXIF/metadata analysis, memory analysis, binary file manipulation, user command history analysis and timelining, file reassembly, steganography, and large file analysis. Currently, this persistent CTF platform has 31 DFIR challenges.

For example, ten challenges titled "Sammy #[1–10]" were created. This set of challenges has the same memory dump from a user named Sammy and students must analyze this RAM (random access memory) to respond to an insider incident. For example, "Sammy #1" contains the memory image to analyze and prepares the students to start the analysis process with volatility as Volatility claims to be the world's most popular framework to extract artifacts from RAM (Volatility Foundation, 2020). All remaining "Sammy" challenges require students to have already identified the correct volatility plugin.

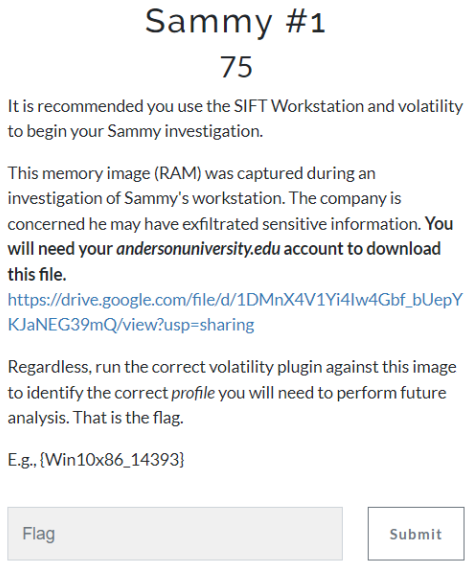


Figure 17. DFIR Challenge Example - 1

The remaining questions help navigate a student through the memory analysis. For example, "Sammy #9" challenges the students to determine a probable location of where Sammy may have escaped to (based on web searches that were extracted from the memory dump).

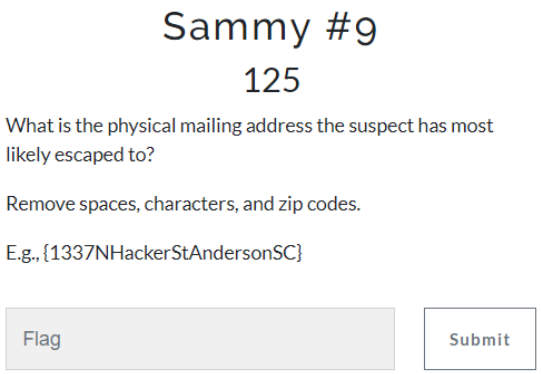


Figure 18. DFIR Challenge Example - 2

5.8 Web

This category contains challenges that require some web server analysis. This includes HTML source code inspections, extraction of files, robots.txt, cookies, SQL injection, cracking web logins, and discovering hidden directories, subdomains, and files. Currently, this persistent CTF platform has 24 web challenges.

For example, a challenge titled "Crack Web Login" was created which contains a password-protected directory on a webserver in the Linode cloud. Students are given authorization and are challenged to crack ctf-user's password on this website. Challenges like this give students a real server to target, scan, and perform hacking activities against.

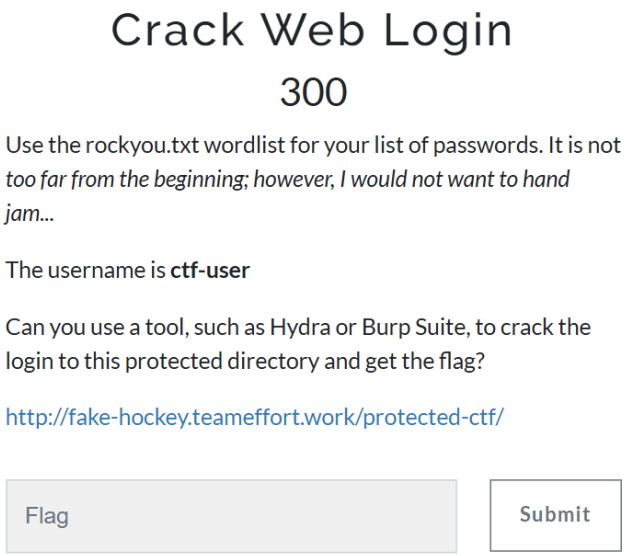


Figure 19. Web Challenge Example

5.9 Miscellaneous

This category contains challenges that require students to complete cybersecurity-related tasks that did not fit well with any of the previous categories. This includes hidden items within an image, manipulating files, answering questions related to cybersecurity talks, social media connections, and virtual machine (OVF) troubleshooting. Currently, this persistent CTF platform has 15 miscellaneous challenges.

For example, a challenge titled "You're Out of Line, Private!" was created where students are given a list of all RFC 1918 private IPv4 addresses (Rekhter et al., 1996). One of the IPv4 addresses in this file is out of numeric order. This challenge requires skills such as scripting and file manipulation, which is why this challenge has been placed in the miscellaneous section.

Figure 20. Miscellaneous Challenge Example

5.10 NCL Archive

A former NCL player from this institution archived prior NCL challenges into this persistent CTF platform. These challenges (as with all ctf.teameffort.work challenges) are only accessible to this institution's cybersecurity students. Archiving challenges within an academic institution has been approved by the National Cyber League. These challenges are not authorized for public posting so an example will not be shown in this work. Currently, this persistent CTF platform has 28 miscellaneous challenges.

6. STUDENT PERSPECTIVE OF THE PERSISTENT CTF PLATFORM

This platform is regularly used as an extracurricular platform during live in-person weekly practices. This platform's institution usually holds two optional practices each week during the semester for either easy or difficult topics. Students are directed to solving challenges on the platform relative to their skillset. The platform is most heavily used by students outside of class or competition practices.

CTF members, after competing in an NCL individual and team competition, were asked, "How did ctf.teameffort.work help you prepare for this competition and/or CTFs in general?" The responses following were received from students that placed in the Top 10% in an NCL Individual or Team competition.

- "The very first CTF challenges I ever completed were on ctf.teameffort.work. The questions were difficult but exciting, and I was hooked. As a freshman without too many technical skills, I started with the OSINT challenges. Since all you really needed for most of these OSINT challenges was access to the Internet, the real challenge lied in thinking outside of the box to find the solution, and I really enjoyed this. I was able to sharpen my problem-solving skills, and as I moved on to other categories of challenges as my technical experience grew, I had a strong foundation to build these new skills on. ctf.teameffort.work continued to serve as a great training ground throughout this process, and the technical difficulty of the challenges on the site was similar to that of most of the

NCL, so I felt prepared when I completed. Overall, in my experience, ctf.teameffort.work was one of the most useful tools in my preparation for CTFs."

- "ctf.teameffort.work helped me prepare for NCL and CTFs in general in a few ways. First, the teameffort.work site was my first introduction to CTFs. It allowed me to 'get my feet wet' and really learn about the format of these competitions as well as the general categories. Second, by practicing on this site, I began building my knowledge base about cybersecurity and CTFs. I was (and still am) able to apply this knowledge to NCL and other CTFs. Finally, by using teameffort.work, I was able to discover what categories I enjoy working on, and more importantly, what categories I needed to improve in. Discovering these weaknesses and categories where I lacked knowledge was critical in improving my scores in NCL and other competitions."
- "It helped me get a better understanding of CTFs overall as well as gave me a place to practice what I've learned in class and apply it to either NCL or CTFs in general!"
- "ctf.teameffort.work has helped me a tremendous amount. Going into this program I had heard about the CTF competition but had no idea how to find any of the solutions. Through this website, I was able to explore and find out how to complete learning objectives in the competitions. This prepared me very well for the NCL and I appreciate it very much."
- "Taught us the concepts needed to succeed in the NCL."
- "It helped me know how to approach CTFs. Practice and learn. But the CTFs can be limited. The web exploitation category is a lot simpler than CTFs from NCL."
- "The OSINT category on the teameffort.work website was very helpful for learning the proper tools and methods for approaching those problems."
- "It helped me learn what certain questions were looking for."
- "Gave me the information related to how a CTF actually functions and what looking for a flag actually means. It also gives an approachable method to exploring the vast catalog of tools that are essential for cyber-related tasks."
- "The website helped me get started and develop my skills in CTFs. It took my small knowledge of Cybersecurity and put me on a fast track to success."
- "The CTF challenges have helped me more than anything when preparing for NCL and other CTFs in general. It breaks down key categories that I see in other competitions like cryptography, web exploitation, network traffic analysis, etc., small chunks that build off of each other. The website, along with practices hosted by [the coach], both help me learn new tools and techniques that I can apply in other competitions, and even some of the classes I'm taking."
- "ctf.teameffort.work helped prepare me for NCL by introducing me to tools that are helpful and vital to solving NCL challenges. To solve many of the ctf.teameffort.work challenges, you have to become familiar with tools that you will most likely also use for NCL. ctf.teameffort.work is very beginner friendly and helped me to go from placing in the top 20% in NCL to top 3.75%! This site is very easy to navigate, as well!"

7. USAGE STATISTICS OF THE PERSISTENT CTF PLATFORM

The persistent CTF platform has 456 challenges across the various categories mentioned previously. 32,141 attempts have been made so far. Of these, 20,508 were incorrect submissions while 11,633 were correct submissions for which points were awarded to the student. These submissions were from 182 students accessing the persistent CTF platform from 1,391 different public IP addresses. Figure 21 shows the percentage of users that have solved each challenge. (Since there are 456 challenges, the name of each challenge is illegible; however, the figure highlights how a majority of the challenges are solved by less than 20 percent of the registered users.)

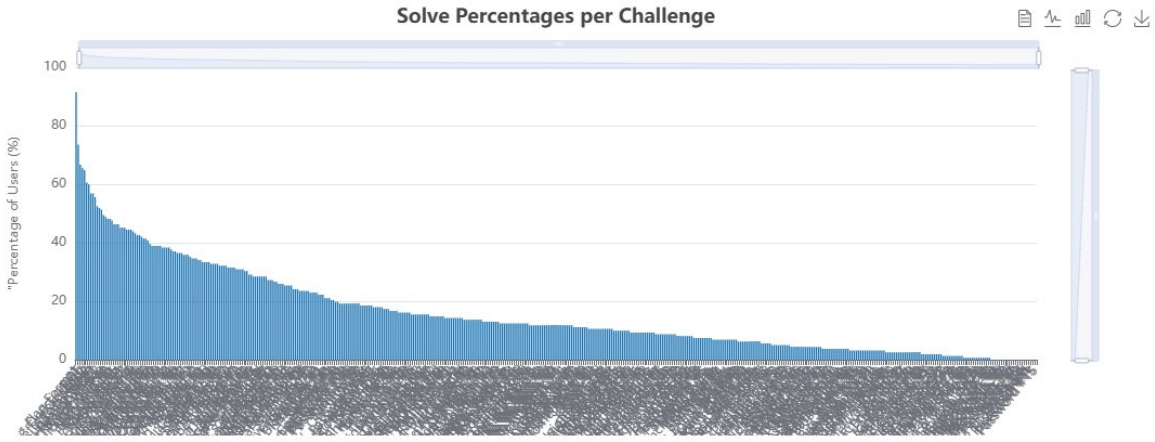
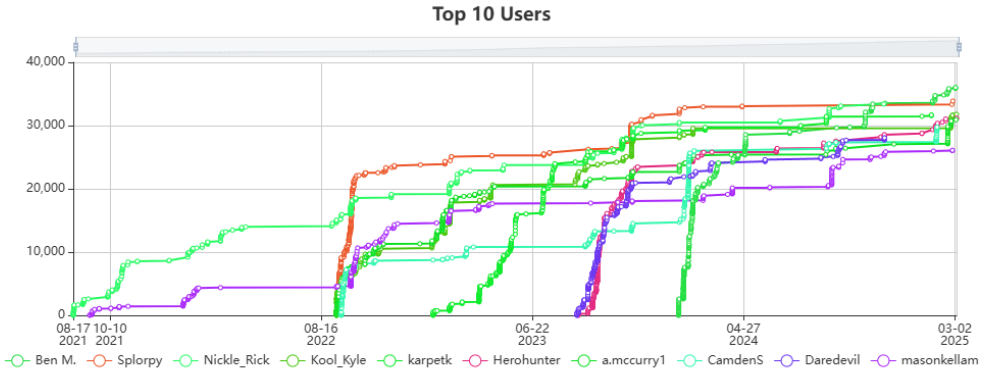


Figure 21. Solve Percentages per Challenge

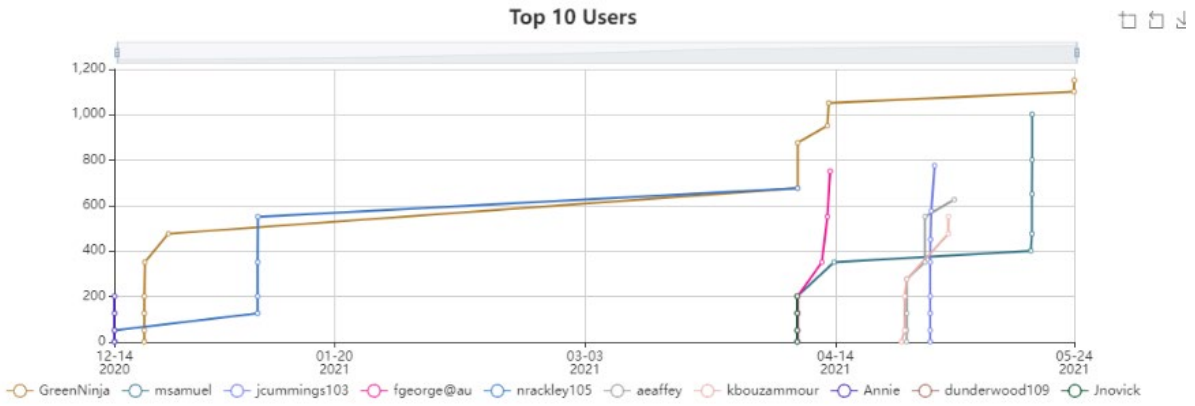
Figure 22 shows the current top 10 students within the CTF scoreboard. The entire results can be found at https://ctf.teameffort.work/scoreboard.



Place	User	Score
1	Ben M.	36020
2	Splorpy	33875
3	Nickle_Rick	33405
4	Kool_Kyle	31780
5	karpetk	31670
6	Herohunter	31185
7	a.mccurry1	30925
8	CamdenS	29765
9	Daredevil	28065
10	masonkellam	26095

Figure 22: Top 10 Users Scoreboard (Current)

The scoreboard has been saved 17 times to the Internet Archive's Wayback Machine between May 31, 2021 and August 11, 2025. This shows the growth of the CTF platform over the past five years. Figure 23 shows the first capture of the CTF platform when only a dozen students participated. All captures can be found at https://web.archive.org/web/*/https://ctf.teameffort.work/scoreboard.



Place	Team	Score
1	GreenNinja	1151
2	msamuel	1001
3	jcummings103	776
4	fgeorge@au	751
5	nrackley105	676
6	aeaffey	626
7	kbouzammour	551
8	Annie	201
9	dunderwood109	201
10	Jnovick	201
11	Mr. Hacker	126
12	nallen	51

Figure 23. Top 10 Users Scoreboard (Archived)

Lastly, the solve count for each challenge can be seen in Appendix B. Some challenges have been available to solve for years while others have been recently created. For example, "Jeremiah 25:26" was one of the original challenges created in December 2020 while "Music Video House" was created in Fall 2024.

8. CONCLUSION

The cost of creating and hosting a persistent CTF platform in the cloud in this research was less than $16 per month. This cost included CTFd software (free), the Linode Ubuntu 24.04 LTS server with 1 CPU Core, 2 GB RAM, and 50 GB Storage at $12 a month with an additional $2.50 a month for backups, and the name registrar monthly cost at less than $1 a month. The persistent CTF has been accessible to all cybersecurity students at this institution since December 2020. In the initial launch, the site had only 15 challenges. During the five years, this website grew to 456 challenges. The motivation to continue adding challenges included: automating the extracurricular education opportunities for the students; giving students a fun and competitive environment to learn and compete; and having a custom internal practice site for the Capture-the-Flag team members to prepare for the National Cyber League (NCL) competition as the NCL claims to be "the most inclusive, performance-based, learning-centered collegiate cybersecurity competition" (National Cyber League, n.d.).

The following table highlights the growth of the Capture-the-Flag participants and performance results after this researcher started using the persistent CTF website for training. This researcher's institution has been ranked as high as #5 (twice) in the United States in the National Cyber League's Cyber Power Rankings. According to the National Cyber League, the NCL's Cyber Power Rankings are a comprehensive measure of the colleges who participate in the National Cyber League. There are 3 factors that are considered in a school's Cyber Power Ranking. In descending magnitude of weight, they are:

- The school's top performing team during the Team Game (4/7 weight)
- The school's top performing student during the Individual Game (2/7 weight)
- The level of participation from the school. Participation level is calculated by counting the number of students who made a submission in the Individual Game with students scoring between 1,000 and 2,000 points counting as two and students scoring 2,001+ points counting as three (1/7 weight)

Semester	Institution Teams	Institution Participants	Top Performing Team (percentile)	Top Performing Individual (percentile)	Institution's NCL Cyber Power Ranking
Spring 2021	1	6	Top 16%	Top 28%	Not Ranked
Fall 2021	1	7	Top 18%	Top 24%	Not Ranked
Spring 2022	2	14	Top 14%	Top 19%	Not Ranked
Fall 2022	5	33	Top 5%	Top 4%	#45 in the Nation
Spring 2023	7	35	Top ~1% *(10th out of 898)*	Top 2% *(48th out of 3,293)*	#9 in the Nation
Fall 2023	7	36	Top 1% *(7th out of 1,050)*	Top 1% *(7th out of 4,236)*	#5 in the Nation
Spring 2024	7	45	Top 1% *(9th out of 1,034)*	Top 1% *(11th out of 3,957)*	#5 in the Nation
Fall 2024	12	46	Top ~2% *(25th out of 1,189)*	Top 1% *(31st out of 4,584)*	#17 in the Nation
Spring 2025	9	52	Top 1% *(9th out of 1,176)*	Top 1% *(8th out of 4,601)*	#6 in the Nation

Table 1. Progression of This Researcher's Institution's NCL Results

This researcher concludes that this low-cost and enjoyable solution has enabled his cybersecurity students to prepare and compete at an extremely high level, especially for a relatively new cybersecurity program.

9. REFERENCES

Barker, C. (2020). *CTF Cryptography for Beginners.* https://charcharbinks.com/post/ctf_crypto_for_beginners/

Bell, S., & Oudshoorn, M. (2018). Meeting the Demand: Building a Cybersecurity Degree Program With Limited Resources. *2018 IEEE Frontiers in Education Conference (FIE)*, 1-7. IEEE. https://doi.org/10.1109/FIE.2018.8659341

Bock, K., Hughey, G., & Levin, D. (2018). King of the Hill: A Novel Cybersecurity Competition for Teaching Penetration Testing. *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. USENIX Association. https://www.usenix.org/conference/ase18/presentation/bock

Boxentriq. (n.d.). *Code-Breaking, Cipher and Logic Puzzles Solving Tools.* https://www.boxentriq.com/

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)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). https://worldcomp-proceedings.com/proc/p2011/SAM5063.pdf

Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024). A Critical Review of Cybersecurity Education in the United States. *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, 241-247. https://doi.org/10.1145/3626252.3630757

Cryptii. (n.d.). *Modular Conversion, Encoding and Encryption Online*. https://cryptii.com/

CTF.zone. (n.d.). *General CTF Information.* https://web.archive.org/web/20210622130946/https://ctf.zone/ctfinfo.html

CTFtime. (n.d.). *What is Capture the Flag?* https://ctftime.org/ctf-wtf/

CTFtime. (2022). *2022 CTF Events* https://ctftime.org/event/list/?year=2022

CTFtime. (2023). *2023 CTF Events* https://ctftime.org/event/list/?year=2023

CTFtime. (2024). *2024 CTF Events* https://ctftime.org/event/list/?year=2024

CyberChef. (n.d.). *A1Z26 Cipher Decode*. https://gchq.github.io/CyberChef/#recipe=A1Z26_Cipher_Decode('Space')

Davis, A., Leek, T., Zhivich, M., Gwinnup, K., & Leonard, W. (2014). The Fun and Future of CTF. *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14).* https://www.usenix.org/system/files/conference/3gse14/3gse14-davis.pdf

dCode.xyz. (n.d.). *About dCode.* https://www.dcode.fr/about

Gonzalez, H., Llamas, R., & Montaño, O. (2019). Using a CTF Tournament for Reinforcing Learned Skills in Cybersecurity Course. *Research in Computing Science*, 148(5), 133-141. https://doi.org/10.13053/rcs-148-5-15

Google Images. (n.d.). *Google Images*. https://images.google.com

Hoffman, P., & Fujiwara, K. (2024). *BCP 219, RFC 9499*. DNS Terminology. https://doi.org/10.17487/RFC9499

Karagiannis, S., Maragkos-Belmpas, E., & Magkos, E. (2020). An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools. *IFIP Advances in Information and Communication Technology*, 61-77. Cham: Springer International Publishing https://doi.org/10.1007/978-3-030-59291-2

Let's Encrypt. (n.d.). *About Let's Encrypt*. https://letsencrypt.org/about/

Linode. (n.d.). *Shared CPU Plans.* https://www.linode.com/pricing/#compute-shared

National Cyber League. (n.d.). *Bridging the Gap from Curriculum to Careers.* https://nationalcyberleague.org

National Cyber League. (2024). *Competition.* https://nationalcyberleague.org/competition

Namecheap. (n.d.). *Domain Prices: Find Popular Top-Level Domains at Unmissable Prices.* https://www.namecheap.com/domains/

Norwood, A. R. (2017). *Grace Hopper.* https://www.womenshistory.org/education-resources/biographies/grace-hopper

PlanetCalc. (n.d.). *A1Z26 Cipher.* https://planetcalc.com/4884/

Public Law 109-163. (2006, January 6). National Defense Authorization Act for Fiscal Year 2006, Sec. 931, Department of Defense Strategy for Open-Source Intelligence. https://www.congress.gov/109/plaws/publ163/PLAW-109publ163.pdf

Raymond, D. (2019, February 13). *Introduction to Capture the Flag (CTF)* [Video]. YouTube. https://www.youtube.com/watch?v=gGeTQsPcTnU

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). Address Allocation for Private Internets. BCP 5, RFC 1918. https://www.doi.org/10.17487/RFC1918

Rober, M. (2018, April 7). *The Super Mario Effect: Tricking Your Brain Into Learning More | Mark Rober | TEDxPenn* [Video]. TED. https://www.ted.com/talks/mark_rober_the_super_mario_effect_tricking_your_brain_into_learning_more

Švábenský, V., Čeleda, 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

Temoshok, D., Fenton, J. L., Choong, Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R., & Richer, J. P. (2025). *SP 800-63B-4 – Digital Identity Guidelines, Authentication and Lifecycle Management*. NIST. https://doi.org/10.6028/NIST.SP.800-63B-4

Thomas, L. J., Balders, M., Countney, Z., Zhong, C., Yao, J., & Xu, C. (2019). Cybersecurity Education: From Beginners to Advanced Players in Cybersecurity Competitions. *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. https://doi.org/10.1109/isi.2019.8823310

TinEye. (n.d.). *Our Mission Is to Make Images Searchable*. https://tineye.com/about

Volatility Foundation. (2020). *Volatility 3 v1.0.0.* https://www.volatilityfoundation.org/3

Wang, P., & D'Cruze, H. (2022). The Role of Cyber Competitions in Cyber Defense Education: A Case Study of National Cyber League (NCL) Participation. *Issues In Information Systems*, 23(3), 128-138. https://doi.org/10.48009/3_iis_2022_111

Wee, J. M. C., Bashir, M., & Memon, N. D. (2016). Self-Efficacy in Cybersecurity Tasks and Its Relationship With Cybersecurity Competition and Work-Related Outcomes. *2016 USENIX Workshop on Advances in Security Education (ASE 16).* https://www.usenix.org/system/files/conference/ase16/ase16-paper-wee.pdf

Zeichick, D. (2024). Confidence and Competence: The Impact of National Cyber League Participation on Career Development in Cybersecurity. *Journal of Computing Sciences in Colleges*, 39(10), 40-47. http://ccsc.org/publications/journals/SW2024.pdf

AUTHOR BIOGRAPHY

Brandon P. Grech is an Assistant Professor of Cybersecurity at Anderson University (SC) where he is also the Cybersecurity Competition Coach. He received his Ed.D. from Liberty University where he researched undergraduate cybersecurity education at Christian institutions. He also has a MS in Cybersecurity and a BS in Computer Networks & Security. He has prior teaching and cybersecurity exercise development experience at CERT/SEI/Carnegie Mellon University. Brandon has authored *100 Linux Commands* and created *316ctf*, a free online cybersecurity CTF program for middle-school and high-school students. Brandon's research interests include cybersecurity education, cybersecurity competitions, and network security.

APPENDICES

Appendix A. CTFd With HTTPS Installation Instructions

These are the installation instructions to install the CTFd platform with HTTPS support. Any command line instructions are in italics.

- Requirements
  - Purchase a Domain Name (Namecheap, etc.)
  - Have an Ubuntu 24.04 LTS with a Public IP address (Linode, etc.)
  - Ensure your purchased domain resolves to your Ubuntu's public IP address. (e.g., the command 'ping ctf-example.teameffort.work' should show your IP address and be reachable)
- Complete the CTFd Docker Install
  - *adduser ctf*
  - *usermod -aG sudo ctf*
  - *su ctf*
  - *cd ~*
  - *sudo apt update*
  - *sudo apt upgrade*
  - *sudo apt install docker.io docker-compose*
  - *git clone https://github.com/CTFd/CTFd.git*
  - *cd CTFd*
  - *head -c 64 /dev/urandom > .ctfd_secret_key*
- Get an HTTPS certificate from Let's Encrypt with the following terminal commands
  - *sudo snap install core*
  - *sudo snap refresh core*
  - *sudo snap install --classic certbot*
  - *sudo ln -s /snap/bin/certbot /usr/bin/certbot*
  - *sudo certbot certonly*
    - Select option 1 (spin up a temporary webserver)
  - Enter your email address
  - Agree to the terms
  - Allow (or not) to share your info
  - Enter domain name (e.g., ctf-example.teameffort.work)
  - Take note of where the certificate and key are saved to
    - E.g. (/etc/letsencrypt/live/ctf-example.teameffort.work/<*.pem>)
- Configure nginx for HTTPS
  - *cd conf/nginx*
  - *mv http.conf https.conf*
  - *vim https.conf*
    - Replace all contents of https.conf with the settings in this example. Ensure to replace the ctf.teameffort.work with your own domain!
  - *cd ../..*
  - *vim docker-compose.yml*
    - The docker-compose.yml contains an nginx section. Ensure it matches this example. Ensure to replace the ctf.teameffort.work with your own domain!
- Start the CTFd instance!
  - *sudo docker-compose up -d*
  - On a desktop machine, open a web browser and navigate to your domain via HTTPS (e.g., https://ctf-example.teameffort.work) and begin setting up the CTFd platform.

These steps are also accessible on GitHub at https://github.com/au-bgrech/CTFd-HTTPS-Install-Steps

Appendix B. Solve Count and Point Values of Each Challenge

Challenge Name	Category	Point Value	Solve Count
DO THIS FIRST! -> Flag Format	OSINT	1	148
Security Question #1	OSINT	50	119
ROT	Crypto	30	108
Search before Cracking	Crypto	25	106
who?	OSINT	50	105
Last Name	OSINT	50	98
Sounds familiar?	Crypto	35	97
Hex Porridge	Crypto	30	92
Real or Fake?	OSINT	75	92
Better than ROT?	Crypto	40	90
Maryland #1	Password Cracking	10	85
who2?	OSINT	50	84
Prime Primes	Crypto	45	83
Unclaimed Property	OSINT	50	80
URL vs IPv4	Network Analysis	25	79
Maryland #2	Password Cracking	10	78
Maryland #3	Password Cracking	10	78
sudo	Log Analysis	50	77
File Starter #1	Log Analysis	10	75
Maryland #5	Password Cracking	15	75
sudo again	Log Analysis	50	75
Maryland #4	Password Cracking	15	73
SHArkba1t! Ooh ha ha! #1	Password Cracking	20	73
Who moved that?	Log Analysis	60	73
Failed Password	Log Analysis	75	72
Maryland #7	Password Cracking	15	72
Numbers	Crypto	40	72
Green E	OSINT	60	71
SHArkba1t! Ooh ha ha! #2	Password Cracking	20	70
File Starter #4	Log Analysis	15	69
Jeremiah 25:26	Crypto	75	69
File Starter #2	Log Analysis	15	68
Cloud Provider	Network Analysis	30	67
Dan? Dan who?	OSINT	75	67
Maryland #6	Password Cracking	15	66
Do You Hear That?	Crypto	50	64
Encoding is not Encryption! Base?	Crypto	50	63
Maryland #8	Password Cracking	20	63
Maryland #9	Password Cracking	20	63
SHArkba1t! Ooh ha ha! #3	Password Cracking	25	63

Challenge Name	Category	Point Value	Solve Count
SHArkba1t! Ooh ha ha! #5	Password Cracking	25	63
Date Night	OSINT	100	62
File Starter #3	Log Analysis	15	62
Symbols #1	Crypto	30	62
Where were you on Nov 1?	Log Analysis	100	62
SHArkba1t! Ooh ha ha! #4	Password Cracking	25	61
Company #1	Current & Past	15	60
SHArkba1t! Ooh ha ha! #6	Password Cracking	25	60
Satellites #1	OSINT	50	59
SHArkba1t! Ooh ha ha! #8	Password Cracking	30	59
Symbols #2	Crypto	30	59
Company #2	Current & Past	15	58
I Saw You Enter...	Log Analysis	150	58
SHArkba1t! Ooh ha ha! #7	Password Cracking	30	58
SHArkba1t! Ooh ha ha! #9	Password Cracking	30	57
... where am I?	OSINT	80	56
Security Question #2	OSINT	75	56
What Country?	OSINT	100	56
First Phone	Crypto	50	55
Symbols #3	Crypto	30	55
90 Ft #1	Crypto	25	54
Self-Signed	Crypto	50	54
Slip and Slide #1	Crypto	25	54
Symbols #6	Crypto	30	54
Collection #1 #1	Crypto	50	53
Company #4	Current & Past	15	53
Military #0	OSINT	50	53
Where were you on Nov 1? #2	Log Analysis	125	53
Numbers #2	Crypto	45	52
Starter PCAP #1	Network Analysis	30	52
Symbols #5	Crypto	30	52
Yet Another BaseXX?	Crypto	50	52
Cloud City?	Network Analysis	35	51
Inspect It	Web	40	51
Inspect It... again	Web	50	51
Starter PCAP #2	Network Analysis	30	51
90 Ft #2	Crypto	30	50
robots.txt	Web	50	50
Starter PCAP #3	Network Analysis	30	50
Symbols #7	Crypto	30	50
Lightswitches	Misc	25	49
Symbols #4	Crypto	30	49

Challenge Name	Category	Point Value	Solve Count
Google Isn't Best	OSINT	80	47
Satellites #2	OSINT	75	47
Company #5	Current & Past	15	46
Favicon	Web	45	46
Published	OSINT	60	46
Starter PCAP #4	Network Analysis	30	46
Starter PCAP #5	Network Analysis	30	46
Tesla Chase	OSINT	80	46
What's on Second?	Log Analysis	125	46
Company #7	Current & Past	15	44
How many attempts?	Log Analysis	100	44
Subdomain	Misc	25	44
Company #3	Current & Past	15	43
Starter PCAP #6	Network Analysis	30	43
Company #6	Current & Past	15	42
Home PCAP #1	Network Analysis	50	42
Old Password?	Crypto	50	42
Click Around	Web	40	41
Dan? Dan who? #2	OSINT	85	41
Starter PCAP #8	Network Analysis	30	41
Where's the salt?	Crypto	50	41
Just a Word Doc	DFIR	60	39
Netflix Autoplay	OSINT	125	39
Satellites #4	OSINT	75	39
Commercial	Current & Past	30	38
Company #9	Current & Past	15	38
EXIF	DFIR	50	38
Satellites #3	OSINT	75	38
Starter PCAP #9	Network Analysis	30	38
Find the Kids!	OSINT	150	37
Sammy #2	DFIR	75	37
who3?	OSINT	75	37
You Know Her... Right?	Current & Past	75	37
Blockchain #1	Crypto	35	36
Facebook #1	Web	75	36
Symbols #8	Crypto	30	36
Old Page	OSINT	75	34
Sammy #3	DFIR	75	34
Third Phone	Misc	60	34
Sammy #1	DFIR	75	33
Sammy #4	DFIR	75	33
Company #10	Current & Past	15	32

Challenge Name	Category	Point Value	Solve Count
Starter PCAP #10	Network Analysis	35	32
DO THIS FIRST!!!	NCL Archive	4	31
High Password #01	Password Cracking	50	31
High Password #02	Password Cracking	50	31
High Password #03	Password Cracking	50	31
Huntsville #1	Password Cracking	40	31
NPS	OSINT	100	31
Sammy #5	DFIR	75	31
Sammy #8	DFIR	125	31
Sammy #9	DFIR	125	31
Security Question #3	OSINT	150	31
90 Ft #3	Crypto	50	30
ac.edu	Network Analysis	60	30
Art?	Misc	50	30
High Password #04	Password Cracking	60	30
Is Water Wet?	OSINT	100	30
Milkshake	OSINT	175	30
Beautiful Bridge Area	OSINT	550	29
Company #11	Current & Past	30	29
Sammy #6	DFIR	125	29
Some Logo	OSINT	100	29
Starter PCAP #7	Network Analysis	30	29
Dog	OSINT	35	28
Sammy #7	DFIR	125	28
Shut the Door!	OSINT	175	28
Facebook #2	Web	100	27
Huntsville #2	Password Cracking	40	27
Huntsville #3	Password Cracking	40	27
Prior Work	OSINT	100	27
90s	Crypto	50	26
Follow That Coin! #1	Crypto	75	26
haxor #1	Crypto	35	26
Huntsville #4	Password Cracking	40	26
Sammy #10	DFIR	125	26
What are you looking at?	DFIR	150	26
Adding Numbers #1	Password Cracking	125	25
Arrested?	OSINT	125	25
CVE	Network Analysis	75	25
Find Her	OSINT	400	25
Huntsville #5	Password Cracking	40	25
Huntsville #6	Password Cracking	40	25
My Original Mentor	OSINT	350	25

Challenge Name	Category	Point Value	Solve Count
Never Enough For Some	OSINT	175	25
What's for Lunch?	OSINT	225	25
Crack the PIN	Crypto	100	24
Huntsville #7	Password Cracking	40	24
Make Your Own Salted Password	Crypto	100	24
Slip and Slide #2	Crypto	40	24
TeamEffort #0	Web	60	24
That's Not Mine...	DFIR	75	24
You Cannot Find Me...	OSINT	500	24
Adding Numbers #2	Password Cracking	125	23
Art? #2	Misc	50	23
EXIF-Store	OSINT	175	23
Family Picture	OSINT	100	23
Greek (OSINT, 2023)	NCL Archive	75	23
Huntsville #8	Password Cracking	40	23
Huntsville #9	Password Cracking	40	23
Past Code #1	Current & Past	40	23
Penguins	OSINT	125	23
Adding Numbers #3	Password Cracking	125	22
Adding Numbers #4	Password Cracking	125	22
Baby Boy	OSINT	125	22
Bird	OSINT	35	22
Military #1	OSINT	150	22
Past Code #2	Current & Past	40	22
Security Question #8	OSINT	200	22
Stone Reminder	OSINT	325	22
What Street?	OSINT	100	22
90 Ft #4	Crypto	60	21
Central Texas #1	Password Cracking	50	21
Central Texas #2	Password Cracking	50	21
haxor #2	Crypto	50	21
I tried... can you fix this?	Crypto	60	21
Login Attempts	Crypto	75	21
TeamEffort #4	Web	70	21
Who took that pic?	OSINT	375	21
Adding Numbers #6	Password Cracking	125	20
Central Texas #3	Password Cracking	50	20
Central Texas #4	Password Cracking	50	20
Central Texas #6	Password Cracking	50	20
Country Wide	OSINT	100	20
CVSS	Network Analysis	100	20
Discord	OSINT	100	20

Challenge Name	Category	Point Value	Solve Count
Find IPv4 Address	Network Analysis	60	20
Find MAC Address	Network Analysis	60	20
Gain Physical Access	Misc	75	20
NFL Record	OSINT	425	20
Say Yes to the Best #4	Password Cracking	75	20
TeamEffort #1	Web	60	20
TeamEffort #3	Web	70	20
Adding Numbers #5	Password Cracking	125	19
Bits & Pieces 1	DFIR	50	19
Book #1	Web	100	19
Central Texas #5	Password Cracking	50	19
Company #8	Current & Past	15	19
Extract Cookies	Web	125	19
Find the Difference	Misc	40	19
It's a Great Day, Like Always	Password Cracking	75	19
OSINT Hunt	OSINT	200	19
Say Yes to the Best #1	Password Cracking	75	19
Say Yes to the Best #2	Password Cracking	75	19
Say Yes to the Best #3	Password Cracking	75	19
Say Yes to the Best #5	Password Cracking	75	19
Say Yes to the Best #6	Password Cracking	75	19
Say Yes to the Best #7	Password Cracking	75	19
Say Yes to the Best #8	Password Cracking	75	19
Say Yes to the Best #9	Password Cracking	75	19
Small Town	OSINT	250	19
TeamEffort #7	Web	75	19
Waypoints (OSINT, 2023)	NCL Archive	100	19
WiGLE #1	Network Analysis	100	19
Aerial View	OSINT	125	18
Central Texas #7	Password Cracking	50	18
Central Texas #8	Password Cracking	50	18
Central Texas #9	Password Cracking	50	18
Security Question #6	OSINT	175	18
What Did You Do This Weekend?	OSINT	525	18
Yet Another /etc/shadow Line	Crypto	75	18
Basketball in What Neighborhood?	OSINT	150	17
Benghazi	OSINT	200	17
Home PCAP #4	Network Analysis	50	17
Hotel Flag	OSINT	150	17
Key is Grid	Crypto	125	17
Krebs & Tweets	OSINT	175	17
Mask #1	Password Cracking	75	17

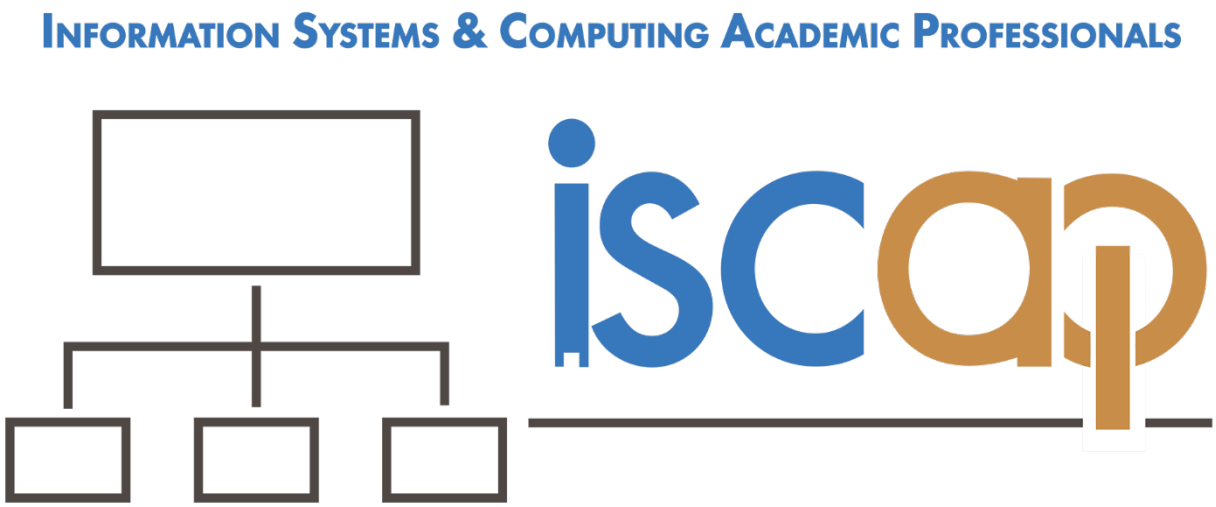
Challenge Name	Category	Point Value	Solve Count
Mask #2	Password Cracking	75	17
Mask #3	Password Cracking	75	17
Mask #4	Password Cracking	75	17
Mask #5	Password Cracking	75	17
Security Question #4	OSINT	175	17
Crack Web Login	Web	300	16
Esoteric (OSINT, 2023)	NCL Archive	100	16
Haircut	OSINT	175	16
High Password #05	Password Cracking	75	16
Home PCAP #3	Network Analysis	50	16
Let the Kids Play	OSINT	125	16
New Neighbor?	OSINT	150	16
Rice Building	Misc	100	16
Book #2	Web	100	15
Cryptocurrency Burning	Crypto	125	15
Down the Block	OSINT	175	15
Global #1	Password Cracking	85	15
Hacker Passwords #1	Password Cracking	75	15
Hidden Image	DFIR	75	15
Home PCAP #5	Network Analysis	50	15
Load Balancing	Network Analysis	75	15
Mask #6	Password Cracking	75	15
Special People. Heroes 4 Sure.	OSINT	325	15
TeamEffort #2	Web	60	15
TeamEffort #6	Web	75	15
Adding Numbers #8	Password Cracking	150	14
Adding Numbers #9	Password Cracking	150	14
Bust the Directories	Web	75	14
Doors	OSINT	600	14
Extract Creds	Network Analysis	100	14
Global #5	Password Cracking	85	14
High Password #06	Password Cracking	75	14
Mask #7	Password Cracking	75	14
More Inspections	Web	100	14
Second Phone	Crypto	60	14
Adding Numbers #7	Password Cracking	125	13
CVE-2	Network Analysis	75	13
Extract String	Network Analysis	125	13
Hacker Passwords #2	Password Cracking	75	13
Home PCAP #2	Network Analysis	50	13
Mint	OSINT	250	13
Where in the World?!	OSINT	575	13

Challenge Name	Category	Point Value	Solve Count
WiGLE #2	Network Analysis	100	13
Crack Encrypted 7-Zip	Crypto	250	12
Find Updates	Network Analysis	60	12
High Password #07	Password Cracking	100	12
Magic Bytes	DFIR	175	12
Satellites #5	OSINT	125	12
Statewide #2	Password Cracking	125	12
Statewide #5	Password Cracking	125	12
TeamEffort #5	Web	75	12
WiGLE #3	Network Analysis	100	12
3 Energy Drinks	OSINT	175	11
Create Your Own Wordlist	Crypto	300	11
Great-Grandpa	OSINT	325	11
Mangle	Crypto	250	11
One Frame	DFIR	100	11
Redaction	DFIR	50	11
Reddit	OSINT	125	11
Remove Hex	Misc	100	11
Statewide #1	Password Cracking	125	11
Statewide #4	Password Cracking	125	11
Traffic View	OSINT	150	11
Work Trip	OSINT	225	11
Extract Web Page	Network Analysis	100	10
Find The Creds	Network Analysis	125	10
Find the Possible Arson	OSINT	250	10
Global #2	Password Cracking	85	10
Global #4	Password Cracking	85	10
Home PCAP #8	Network Analysis	50	10
Home PCAP #9	Network Analysis	50	10
Netcat File Transfer & Examination	DFIR	175	10
What Key Is That In?	DFIR	80	10
WiGLE #4	Network Analysis	100	10
Yet Another Filename Finder	Web	200	10
haxor #3	Crypto	150	9
High Password #08	Password Cracking	200	9
IOC/IoC	DFIR	125	9
Jefferson #1	Crypto	50	9
Security Question #5	OSINT	175	9
Adapting to Change	Crypto	125	8
Docker 1 (Scanning, 2023)	NCL Archive	125	8
Military #3	OSINT	250	8
nc	Network Analysis	50	8

Challenge Name	Category	Point Value	Solve Count
Sq Ft	OSINT	175	8
Statewide #3	Password Cracking	125	8
The Flag To This	Crypto	50	8
What's My Account?	OSINT	200	8
Who is this?	OSINT	550	8
Casting Crowns	Misc	125	7
Collection #1 #2	Crypto	150	7
Docker+FTP	Network Analysis	100	7
Extract Stego	Network Analysis	200	7
Good Ol' Days	OSINT	125	7
High Password #09	Password Cracking	200	7
Home PCAP #6	Network Analysis	50	7
Military #2	OSINT	200	7
Numbers (OSINT, 2023)	NCL Archive	300	7
Password Cracking Country Wide	Crypto	275	7
Rumored Neighbor	OSINT	225	7
Statewide #6	Password Cracking	125	7
Statewide #9	Password Cracking	125	7
Them Bytes	DFIR	100	7
Vantage Point (OSINT, 2023)	NCL Archive	200	7
Aunts&Uncles	OSINT	375	6
Build Your Own Flag	DFIR	200	6
Docker 3 (Scanning, 2023)	NCL Archive	125	6
Follow That Coin! #2	Crypto	80	6
Geolocation Riddle	OSINT	150	6
Jefferson #2	Crypto	55	6
Jefferson #3	Crypto	65	6
Large Image Analysis	DFIR	400	6
PDF (Password, 2023)	NCL Archive	100	6
Statewide #7	Password Cracking	125	6
Statewide #8	Password Cracking	125	6
Voter Registration	OSINT	150	6
You're Out of Line, Private!	Misc	125	6
Arthur #3	Password Cracking	100	5
Arthur #5	Password Cracking	125	5
Arthur #6	Password Cracking	125	5
Arthur #9	Password Cracking	175	5
Bits & Pieces 3	DFIR	125	5
Blockchain #2	Crypto	50	5
Different Flags	DFIR	275	5
Docker 2 (Scanning, 2023)	NCL Archive	125	5
Docker 4 (Scanning, 2023)	NCL Archive	125	5

Challenge Name	Category	Point Value	Solve Count
Docker 5 (Scanning, 2023)	NCL Archive	125	5
Flight Record (Log, 2023)	NCL Archive	150	5
Global #6	Password Cracking	85	5
GPS Coordinates	OSINT	225	5
Ground Floor (Enum, 2023)	NCL Archive	200	5
History 101	DFIR	175	5
Sarah's Vehicle	OSINT	625	5
SQL Injection	Web	450	5
Arthur #1	Password Cracking	100	4
Arthur #7	Password Cracking	175	4
b64 Script	Misc	200	4
Bad Certificate Chain	Crypto	275	4
Banner	OSINT	100	4
Beep Boop (Crypto, 2023)	NCL Archive	250	4
Book #3	Web	100	4
Chunked (Network, 2023)	NCL Archive	100	4
Collection #1 #4	Crypto	250	4
High Password #12	Password Cracking	400	4
Line Drive	Crypto	150	4
LinkedIn	Misc	150	4
Logic Gate	DFIR	250	4
Rolling (Crypto, 2023)	NCL Archive	150	4
Satellites #6	OSINT	200	4
Shiny Stone (Enum, 2023)	NCL Archive	150	4
Warning Banner	Network Analysis	60	4
AutoCrypt (Crypto, 2023)	NCL Archive	300	3
Blockchain #5	Crypto	100	3
Book #4	Web	100	3
Collection #1 #3	Crypto	225	3
Global #3	Password Cracking	85	3
Global #8	Password Cracking	200	3
OVF Import	Misc	350	3
Restaurant WiFi (OSINT, 2023)	NCL Archive	200	3
Security Question #7	OSINT	200	3
Vault (Enum, 2023)	NCL Archive	200	3
Bits & Pieces 2	DFIR	125	2
Bits & Pieces 4	DFIR	300	2
Collection #1 #5	Crypto	525	2
Energizer Bunny Encrypted File	Crypto	175	2
Global #7	Password Cracking	150	2
High Password #10	Password Cracking	350	2
Music Video House	OSINT	650	2

Challenge Name	Category	Point Value	Solve Count
Ponder (Network, 2023)	NCL Archive	300	2
Security Question #9	OSINT	225	2
Steg (Crypto, 2023)	NCL Archive	150	2
AES (Crypto, 2023)	NCL Archive	400	1
Arthur #10	Password Cracking	400	1
Arthur #2	Password Cracking	100	1
Arthur #4	Password Cracking	125	1
Arthur #8	Password Cracking	175	1
Covert Exfiltration (Network, 2023)	NCL Archive	400	1
Hacker Passwords #3	Password Cracking	100	1
Hidden (Network, 2023)	NCL Archive	300	1
High Password #14	Password Cracking	450	1
Memory (Forensics, 2023)	NCL Archive	500	1
PGP (Log, 2023)	NCL Archive	250	1
Slip and Slide #3	Crypto	125	1
WPA	Password Cracking	250	1
@1 Sauce	Crypto	325	0
Arthur #11	Password Cracking	400	0
Blockchain #3	Crypto	60	0
Blockchain #4	Crypto	75	0
Blockchain #6	Crypto	100	0
Blockchain #7	Crypto	125	0
Blockchain #8	Crypto	125	0
Blockchain #9	Crypto	125	0
Crack His Password	Crypto	325	0
Global #9	Password Cracking	250	0
Hacker Passwords #4	Password Cracking	100	0
Hacker Passwords #5	Password Cracking	125	0
Hacker Passwords #6	Password Cracking	150	0
Hacker Passwords #7	Password Cracking	175	0
Hacker Passwords #8	Password Cracking	200	0
Hacker Passwords #9	Password Cracking	200	0
High Password #11	Password Cracking	350	0
High Password #13	Password Cracking	425	0
High Password #15	Password Cracking	475	0
Home PCAP #7	Network Analysis	50	0
Olmstead	Misc	250	0
SSH+Find	Network Analysis	150	0



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)