Securing Our Future: Reducing Barriers to Cybersecurity Education

Sutton Marks

Maggie L. Walker Governor's School

May 8, 2023

I. Introduction

In an era of rapid digitization, most aspects of daily life have shifted online, exposing countless devices to unforeseen security threats. Cybersecurity industry professionals work tirelessly to ensure that such devices are secure, protecting our personal data from unintended breaches of confidentiality, integrity, and availability. As the world's population gradually forfeits old methods of communication and information access in favor of technology and modernization, the demand for cybersecurity professionals continually increases. According to a 2021 study conducted by (ISC)², the global shortage of cybersecurity professionals is estimated to be 2.72 million people (Cybersecurity Workforce Demand, n.d.). Clearly, there is significant demand for cybersecurity professionals, with a noticeable gap existing between the quantity of available positions and the number qualified people to fill them. Additionally, private-sector organizations spent over $150 billion on cybersecurity in the year 2021, increasing by about 12.4% every year on average (Aiyer et al., 2022). As cybersecurity becomes of greater importance to organizations across the globe, the demand for cybersecurity skills and experience will also increase. Without significant efforts to expand interest in cybersecurity, the number of qualified professionals will not satisfy the rising demand for their services. In order to address this concern, this paper aims to minimize barriers to cybersecurity education by investigating the following question: "What can be done to improve access to and interest in cybersecurity?"

II. Capture the Flag Competitions and Their Relevance in Cybersecurity

During Capture the Flag (CTF) competitions, participants complete challenges related to computer security disciplines in order to receive a text "flag" which is exchanged for points.

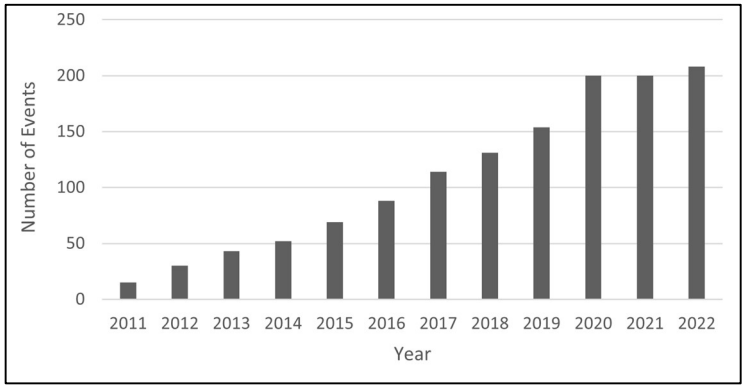
Such competitions are essential in developing the technical, creative, and teamworking skills needed in all aspects of cybersecurity. With challenges in web exploitation, reverse engineering, forensics, cryptography, and many other categories, CTF participants gather vital experience in and a fundamental knowledge of countless cybersecurity topics (CyberTalents, n.d.). Furthermore, participation in such events fosters creativity, teamwork, cooperation, and research, all of which are essential to the problem-solving process common in cybersecurity jobs. While most cybersecurity industry positions don't involve active offensive operations or timed challenges common in CTF events, knowledge of the relevant tools and processes is essential for any position within the field. Not only do CTF challenges provide an opportunity for beginners to learn more about cybersecurity topics, but experienced professionals can also practice with important underlying concepts as well. Furthermore, organizations can use CTF competitions to assess the strengths of their current employees or job applicants. Below are the most common categories found within CTF competitions, the tools frequently used within them, and their relevance to the industry and potential occupations.

Category	**Description**	**Conceptual Understandings**	**Tools**	**Industry-Specific Skills**
Web Exploitation	Finding and exploiting vulnerabilities in web servers	HTML, JavaScript, CSS, PHP, SQL, XSS	BurpSuite OWASP ZAP	Web Programming
Forensics	Extracting information from digital artifacts	Operating systems, file formats, file headers, data carving	Aircrack-Ng Audacity Exif Tool Volatility Wireshark	Operating System and Network Security, Data Manipulation, File Analysis

Reverse Engineering	Analyzing compiled code to determine its purpose, functioning, and vulnerabilities	Assembly language, debuggers, compiling, decompiling	GDB Ghidra BinUtils	Programming, Debugging, "Bounty Hunting"
Cryptography	Using algorithms to decipher encrypted or encoded messages	Asymmetric/Symmetric Key, Advanced Mathematics (Modulo, Exponentiation, Very Large Numbers), Algorithms, Encryption	Python CyberChef	Understanding of Encryption and Data Confidentiality
Network Exploitation	Finding and exploiting vulnerabilities in network services and protocols	DNS, IP, HTTPS, HTTP, SSL, TCP, Certificates, Encryption, Sniffing	Nmap Wireshark	Network Analysis & Security, Intrusion Detection

CTFTime is a popular service used by CTF competition participants to learn about and register for upcoming events. Most public competitions are listed in CTFTime, allowing users to find events and organizers to easily advertise them. CTFTime also provides an API, or Application Programming Interface, with which interested parties can obtain raw data about CTFTime's operations (CTFtime.org / API, n.d.). To assess trends in the popularity of cybersecurity competitions, CTFTime's API was implemented by entering the following URL syntax into a browser: "https://ctftime.org/api/v1/results/[Year]", where [Year] is replaced with the time period of interest. After observing the resulting JSON files generated for the years 2011 to 2022, a graph was created displaying the number of public CTF competitions hosted each year (Figure 1.1). The number of events being hosted has risen gradually over time, suggesting a rise in the popularity of Capture The Flag cybersecurity competitions.

Figure 2.1 – Number of CTF Events Hosted



III. Barriers Faced by Organizers

Despite the popularity of CTF competitions, there remain significant barriers that may impede an organizer's ability and willingness to host them. For example, there are various potential platforms and configuration options from which organizers must choose from. CyberTalents, Facebook CTF, CTFd, Hack the Box, and Root the Box all offer competition frameworks or hosted services. For a first-time organizer, making the most appropriate choice between the platform would require extensive research and experimentation. Furthermore, deciding between different options such as a hosted platform or open-source platform may require an evaluation of the costs associated, presenting an unnecessary and cumbersome burden on the path to hosting a competition.

Additionally, CTF platforms are often expensive, preventing less-funded groups such as school clubs and small businesses from using them. Some platforms, such as CyberTalents and CTFd, can cost over $50 dollars a month, presenting a significant barrier for many prospective organizers. Others, such as Facebook CTF and Root the Box, are much cheaper but difficult to

deploy. Outdated systems and a lack of developer support pose significant barriers to the successful deployment of many competition platforms.

Furthermore, most competition frameworks lack included challenges, forcing the organizers to create such challenges on their own. Those without CTF experience may not know which topics are appropriate to include and as such may face difficulty writing the challenges. The cheaper the platform, the less likely it is to include challenges by default, presenting an unfair barrier to those operating on a smaller budget such as school clubs.

IV. An Analysis of CTF Platform Options

Choosing between the numerous available CTF frameworks can be an arduous task as organizers must weigh countless factors in their decision. To assess the options available, competition planners may need to conduct extensive research, obtain price quotes, experiment with demonstration versions, and gather opinions from others. Furthermore, inexperienced organizers may not know what factors are important to consider when planning a competition. When looking only at price, for instance, organizers may choose a platform that is inexpensive but difficult to deploy or maintain. Therefore, planners must consider several factors when making their decision, weighing each in accordance to how important it is in their particular situation.

In order to simplify the process of choosing a platform, a weighted decision matrix was created for six highly rated CTF frameworks: CyberTalents; Facebook CTF; Hack the Box; CTFd Hosted; CTFd Open Source; and Root the Box (ASQ, 2019). The criteria included in the underlying decision matrix were as follows: Low Price, Appearance, Support, Customizability,

and Ease of Deployment. To create this matrix without the weights applied, online sources including articles, demos, screenshots, and documentation were carefully evaluated. Each platform was assigned a ranking in the categories listed above. A score closer to five within the decision matrix indicates a higher ranking in that category. For example, a "5" within the Price category indicates the lowest price within the selection of platforms. Conversely, a "1" within the Price category indicates the highest price between the platform options. While the below matrix may not necessarily reflect the opinions of every CTF organizer, the rankings reflect the overall consensus of online authors, organizers, and participants based on the sources reviewed.

Figure 4.1 – CTF Platform Decision Matrix without Weights

Platform	Price (Monthly)	Appearance	Support	Customizability	Ease of Deployment
CyberTalents	1	3	4	1	5
Facebook CTF	5	5	1	5	1
Hack the Box	2	4	5	2	4
CTFd Hosted	3	1	3	1	5
CTFd Open Source	5	1	2	4	3
Root the Box	5	2	1	3	2

Next, a field was created for user-specified weights in each of the five categories. The value of each weight corresponds with how important it is to the user. The value in the original matrix was then multiplied by the corresponding weights and displayed in a table. For the weights shown in Figure 4.2 below, the resulting weighted decision matrix is displayed in Figure 4.3. Finally, the weighted values were summed for each platform and the platform with the highest score was determined to be the best fit for the user based on the weighted decision matrix. With the sample weights displayed below, Facebook CTF was determined to be the best-fit platform.

Figure 4.2 – Sample Weights

Category	Ranking
Price (Monthly)	5
Appearance	5
Support	1
Customizable	5
Deployment	3

Figure 4.3 – Resulting Weighted Decision Matrix

Platform	Price (Monthly)	Appearance	Support	Customizability	Ease of Deployment	Total
CyberTalents	5	15	4	5	15	44
Facebook CTF	25	25	1	25	3	79
Hack the Box	10	20	5	10	12	57
CTFd Hosted	15	5	3	5	15	43
CTFd Open Source	25	5	2	20	9	61
Root the Box	25	10	1	15	6	57

To streamline the weighted-decision matrix process for other users, a Java application was created. A Graphical User Interface was included to minimize the need for command line interaction (see Figure 4.4). Within the program, each factor appearing in the original matrix was given a slider ranging from 1 to 5. When the "Submit" button was clicked, the specified weights were applied to the original decision matrix and the platform with the highest resulting score was returned. While an Excel file could provide the same functionality as the Java application, prospective CTF organizers will likely find that the sliders, buttons, and other elements of the interface are easier to use.

Figure 4.4 – Find a CTF Platform GUI

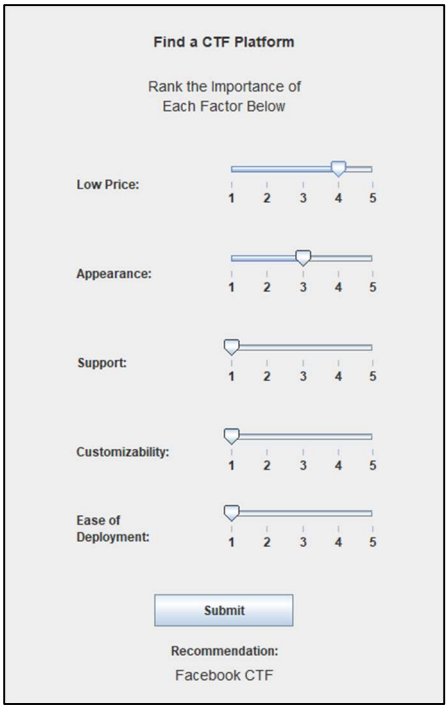


Figure 4.5 – Source Code Outline

1. **Initialize Variables** – assign default values for all variables used in code
2. **createGUI Function** – define slider values, labels, and positions
3. **Change Listeners** – update stored values of sliders when the user changes the slider thumb's position
4. **Button Listener** – reset scores for each platform, call the findCTF function with slider values as arguments, and update recommendation text
5. **findCTF Function** – perform weighted decision matrix calculations

Rather than distributing the file as a raw ".java" file, it was compiled into a single JAR archive and converted into a Windows executable ".exe" file using Launch4j. The most recent release as well as the source code can be retrieved from the GitHub repository at the following link: https://github.com/23smarks/Find-a-CTF-Platform. A brief outline of the source code can also be found in Figure 4.5 above. To execute the application or run the JAR archive directly, Java Development Kit version 20.0.1 or newer must be installed.

To alter the original rankings used in the application, simply open the source code, and make the appropriate changes to lines 14 through 19. Refer to Table 4.6 below for a ranking modification example if necessary. Finally, see the GitHub repository listed above for detailed instructions on how to recompile the code with updated rankings.

Table 4.6 – Sample Code for Modifying The Underlying Decision Matrix

CyberTalents Platform with the Following Rankings: *Price: 2, Appearance: 4, Support: 3,* *Customizability: 2, Deployment: 4*	Facebook CTF Platform with the Following Rankings: *Price: 5, Appearance: 4, Support: 4,* *Customizability: 2, Deployment: 2*
`static Integer[] cyberTalents = new Integer[]{2,4,3,2,4};`	`static Integer[] Facebook CTF = new Integer[]{5,4,4,2,2};`

After experimenting with dozens of slider configurations, Facebook CTF and Hack the Box appeared the most in the results. Based on the original decision matrix, Facebook CTF was ranked as the cheapest option, with the best appearance overall. However, it had the lowest available support and documentation, as well as the greatest difficulty in deployment. Hack the Box was ranked highly in areas that Facebook CTF did not, such as deployment and support. Despite that, however, the costs associated with Hack the Box make it not appropriate for smaller competitions, especially those led by school clubs and other less-funded groups.

By reducing the barriers to Facebook CTF's deployment and thus improving its ranking in that category, Facebook CTF receives the highest overall score in the unweighted decision matrix. Therefore, the matrix suggests that FBCTF is the best option for groups with no specified preferences once deployment difficulties are mitigated. The following section details the deployment issues currently experienced by FBCTF users and seeks to address them accordingly. By removing these barriers to one of the cheapest CTF frameworks available, hosting a CTF competition will become much easier for less funded or inexperienced organizers.

V. Procedure for Converting FBCTF into an Amazon Web Services EC2 Instance

While a standalone installation following the documentation directions is possible, it requires greater familiarity with the Ubuntu Linux operating system and how to operate in a command line environment. Furthermore, outdated packages in the original framework prevent the entirety of the framework from being installed without making significant modifications to system files. This method for deployment seeks to develop a means by which businesses, schools, and extracurricular groups can easily implement the training platform without the skills and experience needed for the standard installation procedure. Additionally, the documentation regarding cloud-based hosting is minimal, and those seeking to deploy the framework in a cloud platform may face difficulty due to its outdated packages and the lack of developer support online. By providing any easy and efficient way to configure the platform in a cloud setting, the method below seeks to eliminate the barriers facing users of the FBCTF framework and provide steps for users of other platforms to deploy cybersecurity training services with minimal difficulty.

Because the platform is no longer actively supported and cannot be installed on modern Linux versions, a virtual machine of the original platform and operating system was obtained from an online source to replicate the structure and quality of the framework. After verifying the security of the files through an antivirus scan, VMware Workstation Player 17 was installed to view and operate the virtual machine. After downloading VMware, it was launched and the FBCTF virtual machine (VM) was imported by locating the ".vmx" file in the original VM download. Next, the platform was launched and logged into using the default credentials "fbctf" as the username and "123" as the password. Entering the command "ifconfig" into the terminal indicated that the service is running at a private IP address, which can only be accessed from within the network. For others to access it, as would be necessary in a large setting such as a business or classroom, the service must be operating on a public IP address which can be accessed from any device. This is best achieved through an Amazon Web Services Elastic Cloud Compute instance, which has minimal costs and high reliability.

To transition the virtual machine into AWS, several tools including VMware's OVFtool and the AWS Command Line Interface were implemented. However, slight modifications to the original machine had to be made in order to guarantee that its functionality is maintained once hosted on AWS. First, Secure Shell (SSH) was enabled on the virtual machine as that will be the only means to connect to the back-end infrastructure once hosted in AWS. SSH is a network protocol for connecting securely to another computer over an otherwise insecure network (Ylonen, n.d.). To determine whether or not Secure Shell was enabled on the instance by default, the following command was executed:

```
ps aux | grep openssh
```

No results were returned, indicating that the service was not running on the instance. Running the following command also returned no results, revealing that the virtual machine did not have SSH server capabilities installed.

```
dpkg -s openssh-server
```

In order to create the functional SSH server needed in AWS, the OpenSSH Server package must be installed. To gather the necessary files and install them within the instance, the following command was run:

```
sudo apt-get install openssh-server
```

To verify that the machine was listening for connections on port 22, the default connection for SSH, the netstat command was executed. The Windows Command Prompt (cmd.exe) was then launched to verify that the virtual machine could be connected to over SSH, as an operating SSH server is essential for AWS migration. In the Windows Command Prompt, the following command was entered, followed by the default password "123" when prompted:

```
ssh fbctf@192.168.178.128
```

Please note that the IP address following the "@" sign is specific to the instance used in this example. In other words, the ifconfig command may be needed to determine the IP address of the host machine since it differs between installations.

After entering the login credentials, the Command Prompt successfully connected to the virtual machine, indicating that the VM was ready to proceed in the migration process.

The next step in the transition from a privately hosted virtual machine into a public Amazon Web Services EC2 instance involved exporting the VM appliance into a format that could be read by AWS. This was accomplished by using VMware's included OVFtool command-

line application, which packages the many disk files contained in the VM into a single OVA file. OVA files, or “Open Virtualization Archives,” are TAR packages containing all the files the virtual machine needs in order to be distributed without losing any information. To begin exporting the virtual machine using OVFtool, the base “.vmx” file of the virtual machine was located. From the main VMware Workstation Player menu, this was accomplished by selecting the virtual machine, choosing “Edit virtual machine settings,” and clicking on “Hard Disk (SCSI).” Then, path to the disk file was copied after removing the “[VMNAME].vmdk” file from the path. This location was opened on the computer being used, and the file ending with a “.vmx” extension was located. Next, name of the “.vmx” file was appended to the original copied path using a text editor, and the resulting path was copied.

In order to use OVFtool, a Command Prompt window must be running with the OVFtool directory as the working location. For Windows computers, this is either “C:\Program Files (x86)\VMware\VMware Player\OVFTool” or “C:\Program Files\VMware\VMware Player\OVFTool” depending on the computer in use. In this case, the OVFTool program was in the former. To begin using OVFtool, the following command was entered into a Command Prompt window, navigating to the directory of the OVFTool.

```
cd C:\Program Files (x86)\VMware\VMware Player\OVFTool
```

Next, OVFTool was executed and the VMX file was converted into an Open Virtualization Archive. To run the command with the correct arguments, the following was entered into the Command Prompt:

```
ovftool [PATH_TO_VMX]\[VMX_NAME].vmx [OUTPUT_PATH]\[OUTPUT_NAME].ova
```

The command arguments [PATH_TO_VMX]\[VMX_NAME].vmx and [OUTPUT_PATH]\[OUTPUT_NAME].ova were replaced with the previously copied path, the intended output destination, and output file name. After pressing Enter, OVFtool began packaging the virtual machine into a single file. Once the command was done running, the new OVA archive was found within the specified output directory

With the OVA archive created, the virtual machine was successfully packaged into a single file and was ready for import into Amazon Web Services. AWS, however, requires "buckets" in which to store imported files. These can be created easily through S3, a scalable storage service provided by AWS and accessible at the following URL: https://s3.console.aws.amazon.com. After navigating to S3 and choosing "Create bucket," the bucket name and region were entered into the prompts. Once the bucket was created, it was opened by clicking on its name within the console. Then, the OVA file was uploaded by choosing "Upload," followed by "Add files." In the case of the FBCTF image, about two gigabytes of bucket storage were used with an upload time of approximately five hours.

Before converting the OVA file into an Amazon Machine Image, a container file must be created in order for the Command Line Interface (CLI) to locate the correct disk file (Importing a VM as an Image Using VM Import/Export, n.d.). Within the bucket created in the previous step, the OVA URI was copied, and the following code appended to a blank "containers.json" file, substituting the URL previously copied URI:

```
[
  {
    "Description": "My Server OVA",
    "Format": "ova",
    "Url": "s3://my-import-bucket/vms/my-server-vm.ova"
  }
]
```

Next, the files were uploaded to AWS CloudShell by selecting “Actions -> Upload File” and choosing the “containers.json” file. Finally, convert the OVA file was converted into an Amazon Machine Image using the following CloudShell command:

```
aws ec2 import-image --description "My server VM" --disk-containers
"file:// containers.json" ⇒
```

The conversion process lasted approximately ten minutes and was monitored using the following command, replacing the last string with the ID given when the import command was initiated.

```
aws ec2 describe-import-image-tasks --import-task-ids import-
ami-1234567890abcdef0 ⇒
```

To employ the FBCTF framework, the steps above are not necessary since they have already been completed. Instead, prospective users can create an EC2 instance using the following AMI ID and name:

```
ID: ami-06eaa3565f4b601d3
Name: import-ami-0db2f46d3d09f4f00
```

To create an AWS EC2 instance running the FBCTF framework, open the “Launch an Instance” menu and enter the above AMI name into the “Application and OS Images” search bar. Next, choose “Community AMIs” and select the only result. Enter the remaining configuration details such as storage capacity and instance type, followed by “Launch Instance.” Connect using the SSH key specified in the instance configuration, as well as the default password “123”. To change the password once connected via SSH, enter the passwd command followed by the new and old passwords when prompted. To verify that the instance is successfully running, enter the IP address into a browser. If everything was configured properly, the text “Conquer the World” should be easily visible.

For those intending to migrate another CTF framework from a virtual machine to the cloud, the steps above should be sufficient in detailing the correct import procedure.

VI. Procedure for Registering a Domain Name and Elastic IP Using AWS

While the FBCTF platform can be accessed using the dynamic public IP address of the EC2 instance, some may find it more convenient to access the service using a domain name. Not only is acquiring a domain name appealing to many organizers, but it is also a necessary step in obtaining an SSL certificate for the platform. The below steps are applicable for any EC2 instance running an NGINX web server.

Before registering and associating a domain with the instance, an Elastic IP address must first be created and linked to the original EC2 instance. In Amazon Web Services, an Elastic IP address is a static replacement for an instance's dynamically changing public IP address. In other words, the instance's IP address is fixed and will never change. To begin creating an Elastic IP, navigate to the EC2 console page at https://console.aws.amazon.com/ec2 and verify that your FBCTF instance is running. Next, locate the "Network & Security" tab on the left side of the console and choose "Elastic IPs." Then, choose "Allocate Elastic IP address" followed by "Allocate." In the resulting notification, click "Associate Elastic IP address" and select the FBCTF instance in the "Choose an instance" search bar. Finally, click "Associate" to link the Elastic IP address to the EC2 instance.

To register a domain name for your instance, navigate to AWS' domain registration service, Route 53, by entering the following URL: https://console.aws.amazon.com/route53. Under the "Register domain" header, enter your requested domain name and select "Check." Choose the domain name and enter payment details to acquire the domain. Wait at least an hour

before navigating to the “Hosted zones” panel in the Route 53 dashboard to ensure that the Route 53 registrar has fully registered your domain.

In the “Hosted zones” panel, select the radio button next to your newly registered domain, followed by the “View details” button. Next, choose “Create record,” followed by “Simple routing.” Select “Define simple record” and choose “A” as the record type. Finally, open the “Choose endpoint” dropdown, select “IP address,” and enter the Elastic IP address in the text box. After selecting “Define simple record,” the EC2 instance should be accessible by entering the domain name in your web browser.

VII. Configuring SSL Certificates Using Let’s Encrypt and Certbot

Secure Sockets Layer, or SSL, is an Internet security protocol that guarantees both traffic encryption and website authenticity. Websites using SSL can be easily identified by examining the open or closed padlock symbol at the left of the URL field. When SSL is in use, a locked padlock appears, signaling to the user that their traffic is secure. In order to verify the authenticity of the website and establish a means for secure communication, SSL requires individual certificates for each website it is implemented on. These certificates must be issued by a “trusted authority” and cannot be written directly by the website administrator. There are many options available, however, for such administrators to obtain an SSL certificate without having to pay money or go significantly out of their way. Let’s Encrypt, for instance, is a nonprofit certificate authority which allows users to easily create SSL certificates without having to pay.

Upon initial observations of the FBCTF framework created in an earlier section, it was determined that an SSL certificate was not in use. To begin the process of obtaining a certificate,

the original GitHub documentation was reviewed. The automated production installation outlined in the GitHub instructions includes a provision script, a series of commands executed by the computer during installation. The provision script included several references to "certbot-auto," a tool used to create SSL certificates using Let's Encrypt as the certificate authority (Installation Guide, Production, n.d.). When the provision script commands were manually entered into the new FBCTF instance, errors were returned to the console explaining that "certbot-auto" could not be found to download. The Certbot documentation available on the Cerbot website explains that certbot-auto is no longer used and only the classic Certbot application is maintained (User Guide — Certbot 2.6.0 Documentation, n.d.).

Combining the Cerbot installation directions with the usage and configuration options required by the FBCTF framework, the following set of commands was created:

```
sudo apt-get install snapd ⇒
sudo snapd install --classic Certbot ⇒
sudo certbot –nginx ⇒
cd /etc/nginx/sites-available ⇒
sudo nano fbctf.conf ⇒
```

This selection of shell commands installs Certbot, executes it using the NGINX option, and opens the FBCTF configuration file for the next step listed below. The NGINX option used in the third command is specific to instances using NGINX, a simple web hosting application, as the primary hosting mechanism. Once the fbctf.conf configuration file was opened, the following was entered as a new line in the server information section, replacing [domain] with the domain name in use:

```
server_name [domain]
```

This entry must be identical to the domain name(s) specified when Certbot was executed. Next, existing certificates were removed, and the Cerbot-generated keys were linked to new files. Finally, the remaining “dhparam” SSL file was created, the NGINX configuration was altered per the directions in the documentation, and the NGINX service was restarted. Below are the commands that were entered:

```
cd /etc/nginx/certs ⇒
sudo rm * ⇒
sudo ln -s "/etc/letsencrypt/live/[domain]/fullchain.pem
/etc/nginx/certs/fbctf.crt || true ⇒
sudo ln -s "/etc/letsencrypt/live/[domain]/privkey.pem"
/etc/nginx/certs/fbctf.key || true ⇒
sudo openssl dhparam -out /etc/nginx/certs/dhparam.pem ⇒
cat /var/www/fbctf/extra/nginx.conf | sed
"s|CTFPATH|/var/www/fbctf/src|g" | sed
"s|CER_FILE|/etc/nginx/certs/fbctf.crt|g" | sed
"s|KEY_FILE|/etc/nginx/certs/fbctf.key|g" | sed
"s|DHPARAM_FILE|/etc/nginx/certs/dhparam.pem|g" | sudo tee
/etc/nginx/sites-available/fbctf.conf ⇒
sudo rm -f /etc/nginx/sites-enabled/default ⇒
sudo ln -sf /etc/nginx/sites-available/fbctf.conf /etc/nginx/sites-
enabled/fbctf.conf ⇒
sudo nginx -t ⇒
sudo service nginx restart ⇒
```

After the final command was executed and the instance was rebooted, the closed padlock appeared next to the domain name, indicating that the SSL certificate had been successfully deployed. As a result, users of the FBCTF platform will have their network traffic encrypted

when visiting the site. To implement SSL certificates on another FBCTF installation, follow the above steps and replace user-specific values such as the domain name when appropriate.

For instructions on how to add challenges to a Facebook CTF instance, view the original documentation at the following link: https://github.com/facebookarchive/fbctf/wiki/Admin-Guide. Challenge files updated regularly and available for public use are located at the following link: https://github.com/23smarks/ctf-challenges.

VIII. Conclusion

Because of its low cost and high customizability, FBCTF is ideal for audiences such as school clubs or small businesses with little experience hosting CTF competitions. By eliminating the deployment difficulties facing prospective users of the FBCTF framework, organizers are now able to actively deploy it with minimal hardship. For less-funded organizers, the reappearance of FBCTF as a CTF framework option will likely lead to more competitions at the educational and small business levels over time. In turn, more students and professionals will obtain the skills and interests necessary for a career in cybersecurity. For those interested in other platforms besides FBCTF, the weighted decision matrix application mentioned previously will allow for organizers to quickly make the best choice given their preferences. By minimizing the barriers facing organizers of cybersecurity competitions, namely framework availability, decision-making, and cost, they will find choosing, configuring, and deploying a platform to be much easier. Enhancing access to cybersecurity resources, as outlined in this paper, will undoubtedly have a positive impact on the next generation of cybersecurity professionals by providing them with the knowledge, skills, and interests needed to succeed.

References

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022, October 27). *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers | McKinsey*. Www.mckinsey.com. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

ASQ. (2019). *What is a Decision Matrix? Pugh, Problem, or Selection Grid | ASQ*. Asq.org. https://asq.org/quality-resources/decision-matrix

CTFtime.org / API. (n.d.). Ctftime.org. Retrieved May 10, 2023, from https://ctftime.org/api/

Cybersecurity Workforce Demand. (n.d.). https://www.nist.gov/system/files/documents/2022/07/06/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf

CyberTalents. (n.d.). *Getting Started in Capture the Flag (CTF) Competitions*. CyberTalents Blog. https://cybertalents.com/blog/getting-started-in-capture-the-flag-ctf-competitions

Importing a VM as an image using VM Import/Export - VM Import/Export. (n.d.). Docs.aws.amazon.com. Retrieved May 10, 2023, from https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html

Installation Guide, Production. (n.d.). GitHub. https://github.com/facebookarchive/fbctf/wiki/Installation-Guide

User Guide — Certbot 2.6.0 Documentation. (n.d.). Eff-Certbot.readthedocs.io. Retrieved May 10, 2023, from https://eff-certbot.readthedocs.io/en/stable/using.html

Ylonen, T. (n.d.). *What is SSH (Secure Shell)?* Www.ssh.com. https://www.ssh.com/academy/ssh