**Cyber Range User Guide**

By NAC-ISSA



# A Word from the Project’s Lead Developer…

Welcome to the NAC-ISSA Cyber Range. We are glad you’ve chosen to spend some time with us!

Our Cyber Range began as an idea in the summer of 2018 and has grown through community support. We would not be where we are without the support of many people in the Cyber community. Especially NAC-ISSA. Great credit belongs to the board for placing their trust in me as we spent about $10,000 in hardware to realize a dream. Our premise was simple- provide a platform for CTF competition and provide a way to train others in the greater Huntsville Cyber Community. We developed our platform intially with the idea that it should be portable and would not require internet access to run. We would bring the training to you. When the Covid-19 pandemic struck we once again rolled up our sleeves and re-thought how we would offer Cyber Range services to a population that was staying home. It caused some minor changes but we had already built upon a solid concept and used Apache Guacamole to provide remote access services. We were able to pivot on that concept and can now offer the Cyber Range in person or remotely. The choice is up to you. We hope you enjoy our platform and will spend some time exploring what it has to offer.

Sincerely,

Jeremy Tourville

Lead Cyber Range Developer, RHCSA

NAC-ISSA Equipment Director

# Using the Cyber Range

Welcome to the Official NAC-ISSA Cyber Range! We appreciate the opportunity to assist you as a training partner along your journey to becoming a Cyber Security professional. In addition to free training, the NAC-ISSA Cyber Range is home to many rigorous and rewarding CTF challenges. So, while you may have first encountered the Cyber Range at one of our local CTF challenges such as the annual Rocket Secure, please stick around to enjoy some of the hands-on labs that our knowledgeable development staff has put together for our benefit.

# Requesting Initial Access

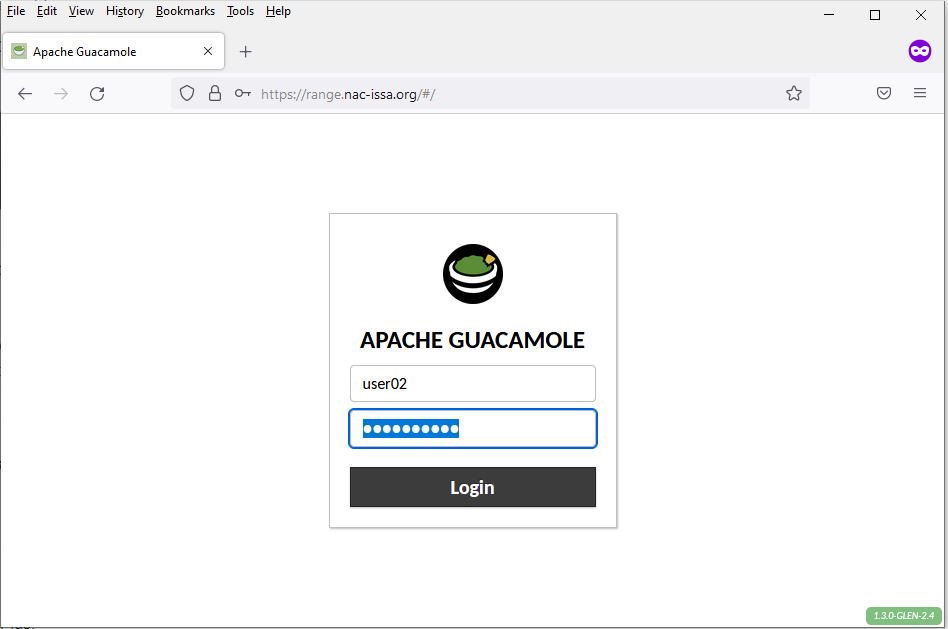
To access the Cyber Range as a student or Capture-the-Flag contestant, please follow the instructions listed below with respect to your activity. If you are interested in the continued development of the NAC-ISSA Cyber Range and would like to assist, please contact our Lead Developer, Jeremy Tourville, using the following email address: [Jeremy.Tourville@nac-issa.org](mailto:Jeremy.Tourville@nac-issa.org). In addition to reaching out directly, keep an eye out for opportunities to collaborate with our staff by registering for any of our upcoming Cyber Range Development meetings. These meetings, as well as any upcoming Capture-the-Flag events, can be found on the event page of the NAC-ISSA website which can be found at https://nac-issa.org/NAC\_Events.asp?Grid=All.

# Accessing CTF Challenges

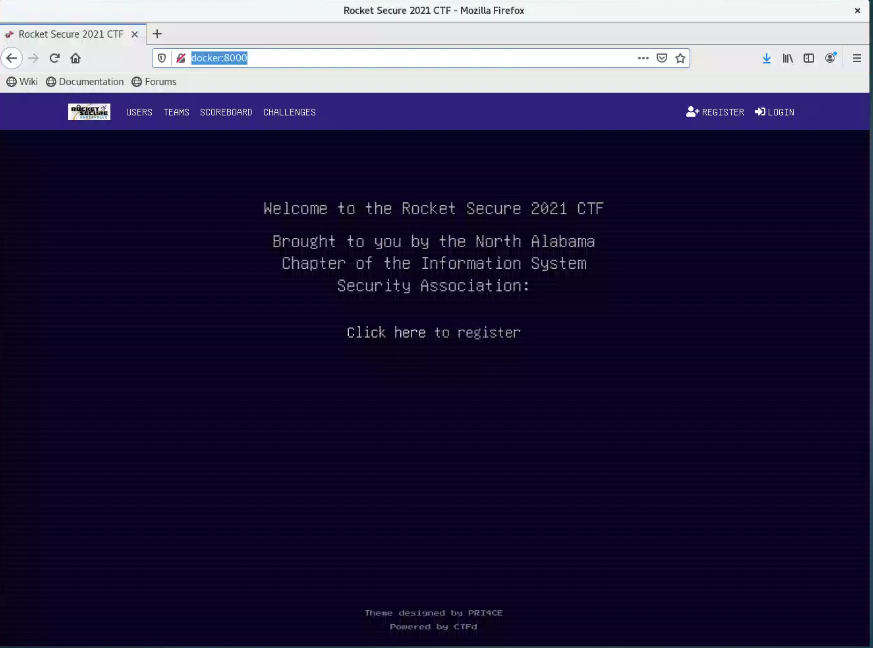
Capture-the-Flag competitions are not solely about who can best navigate the CLI with ease and agility. Successful contestants must know when to use the appropriate offensive tactics, techniques, and procedures to analyze (and eventually exploit!) weaknesses in a given virtual environment. Contestants are given a Kali Linux desktop tasked with finding clues and hidden keys within various target systems called “flags”. These flags can be hidden in Javascript, stored as encoded text inside a browser cookie, or may simply be stored within a text file. Users must discover these flags by following clues which are also hidden inside each challenge. Once a flag is located within the target system, the user will return the uncovered flag’s value in order to earn points. The winner of the CTF challenge is the team with the most points at the end of the day.

1. Upon arriving at the event, you should be greeted by the CTF Coordinators and assigned to an available laptop. This laptop will be assigned to a particular Device ID which you should use to login and complete any challenges.
2. Using the supplied Device ID, log into the device’s user account using the below credentials:
   * **Username**: user<<device ID>>
   * **Password**: Password12

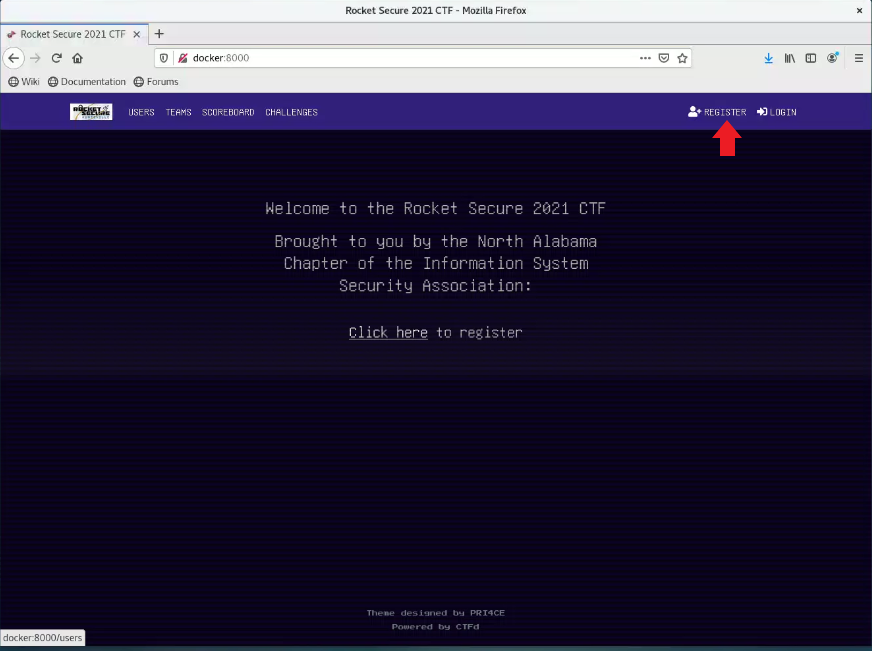
For example, if your laptop is labeled with Device ID #2 then you will login using the username ***user02***. If your laptop is labeled with Device ID #13 then you will login using the username ***user13***. The password for your user account will be ***Password12***. Please see the picture below.



1. Once logged into your attack machine’s user profile, you should arrive at a fresh installation of a Kali Linux desktop.
2. To locate the CTF challenges, open the Firefox ESR application. This can be found by clicking the Kali Linux icon in the upper-left corner of your desktop and typing “firefox” into the search bar.
3. Once the Firefox browser is open, locate CTF Home Page by navigating to ***docker:8000*** in the URL search bar.

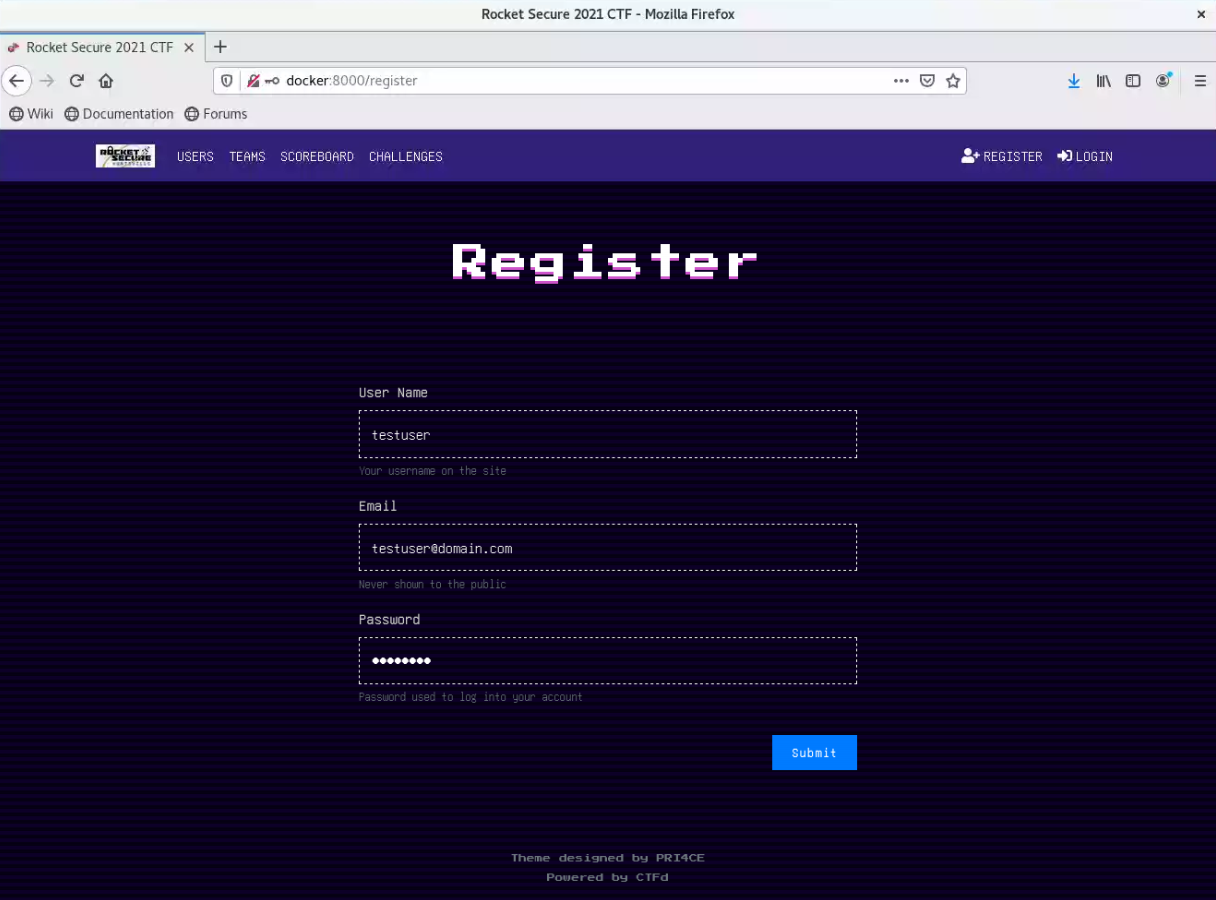


1. Once you land on the CTF Home Page, you must login using your existing CTF user credentials or create an account. Let’s walkthrough creating a user account by selecting “Register” in the upper-right corner of the page’s navigation bar.

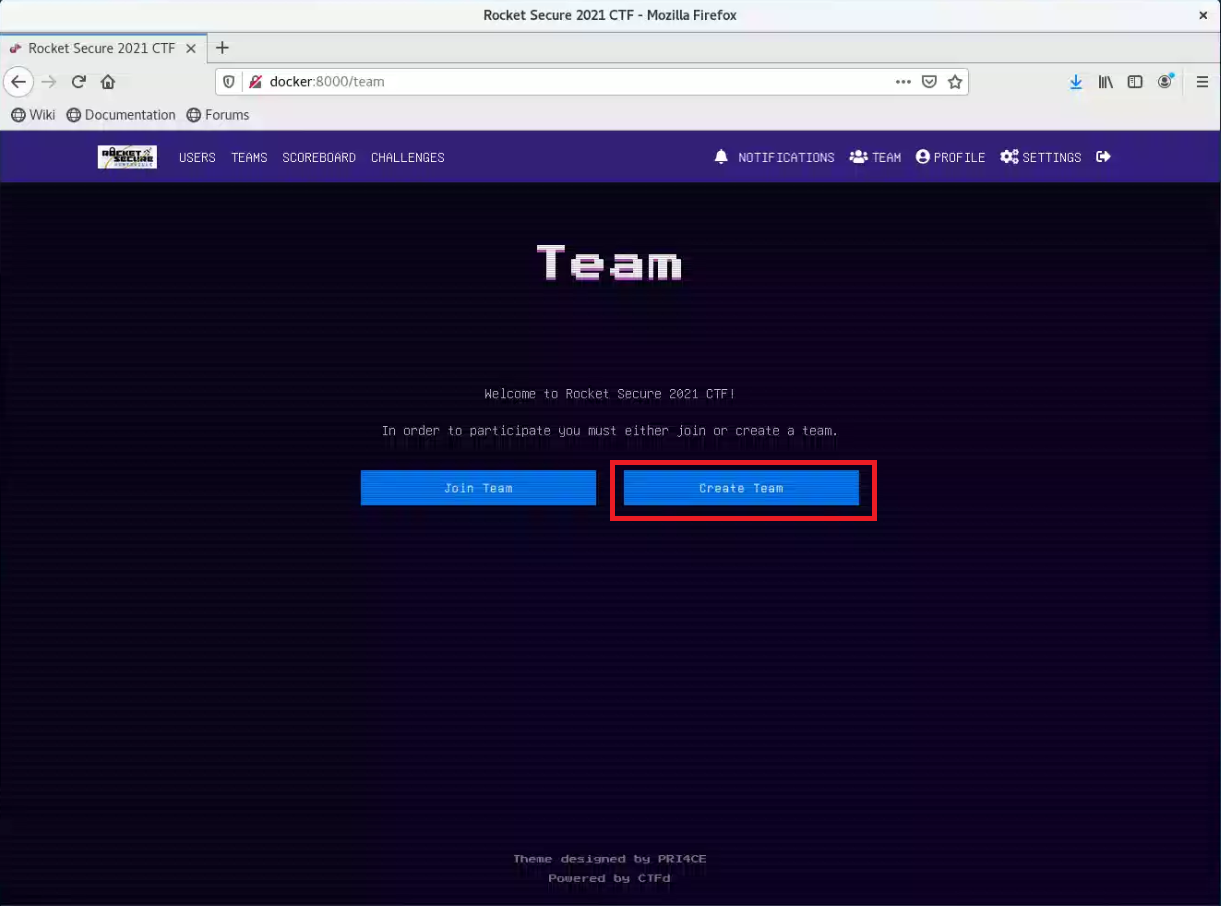


1. Next you will need to create your user account for the event by entering your selected username, email address, and password. This will be the user account that you use to access challenges and score points for your team, which we will create momentarily.

**Please note that we will never share your email address with anyone outside of our organization. PERIOD!!!**

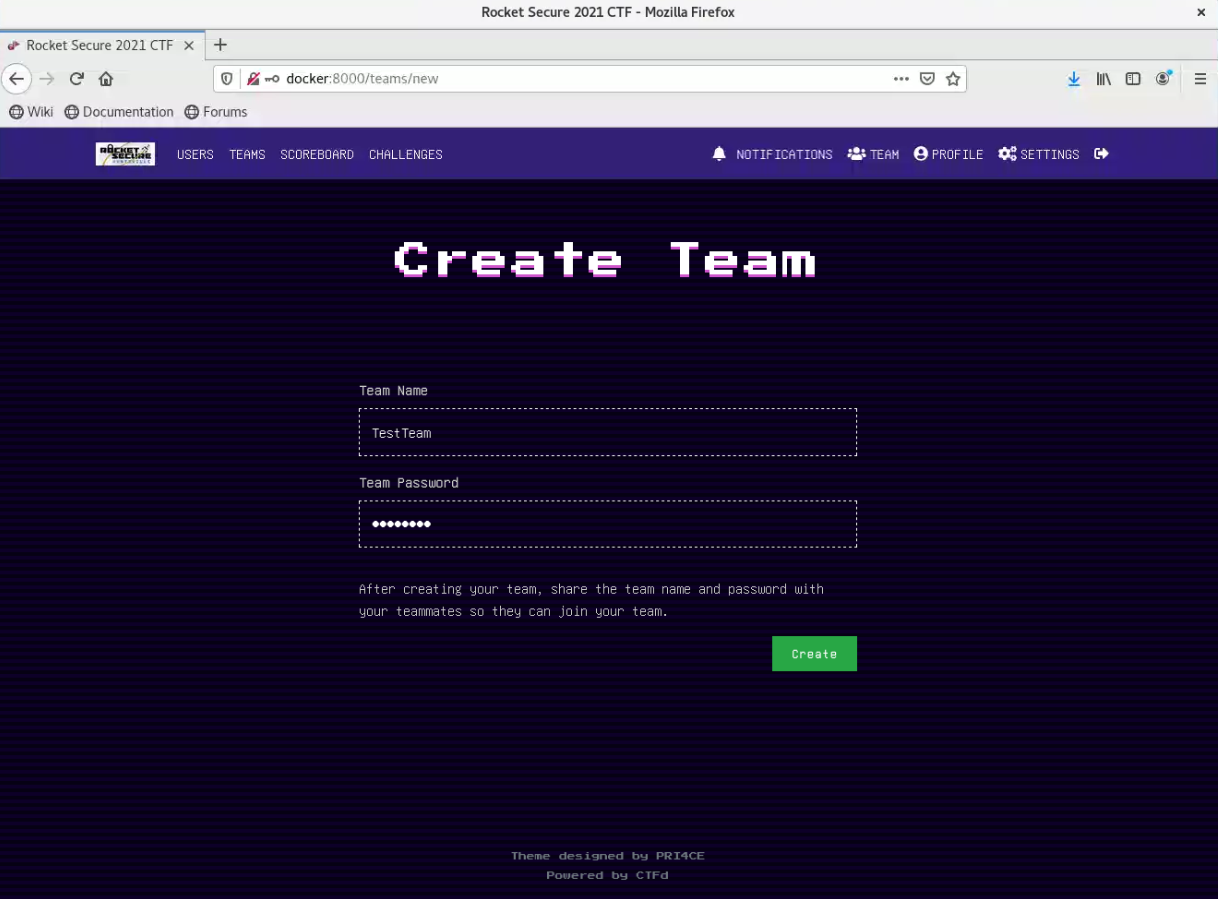


1. After creating a user account, you must either Join or Create a Team. Let’s begin by creating a team. To create a team, select the “Create Team” option.

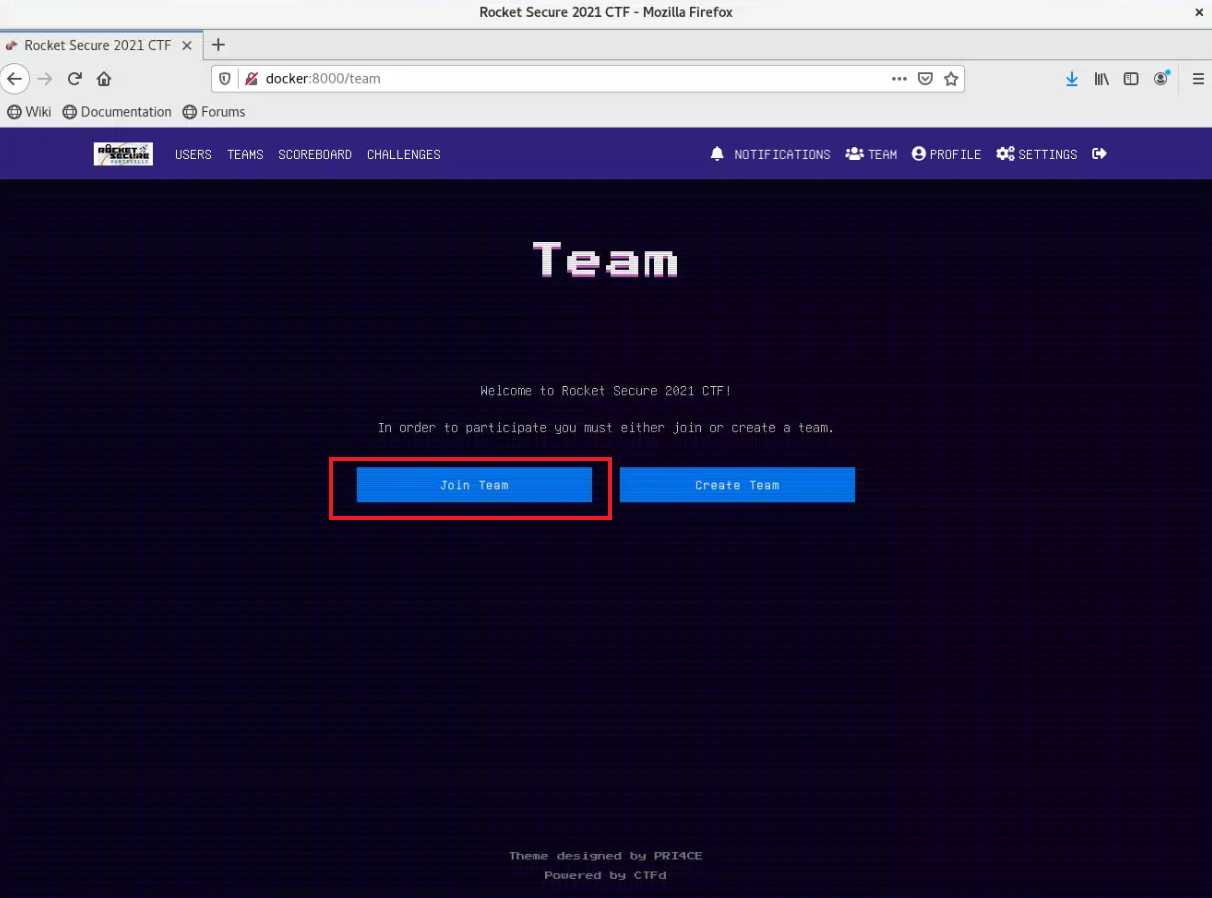


1. To create a team, you will first be asked to create a name for your team. After entering a Team Name, you will be asked to create a password to join your team. Fill out your team details, select the green button labeled “Create”. This will make your team live for other users to join.

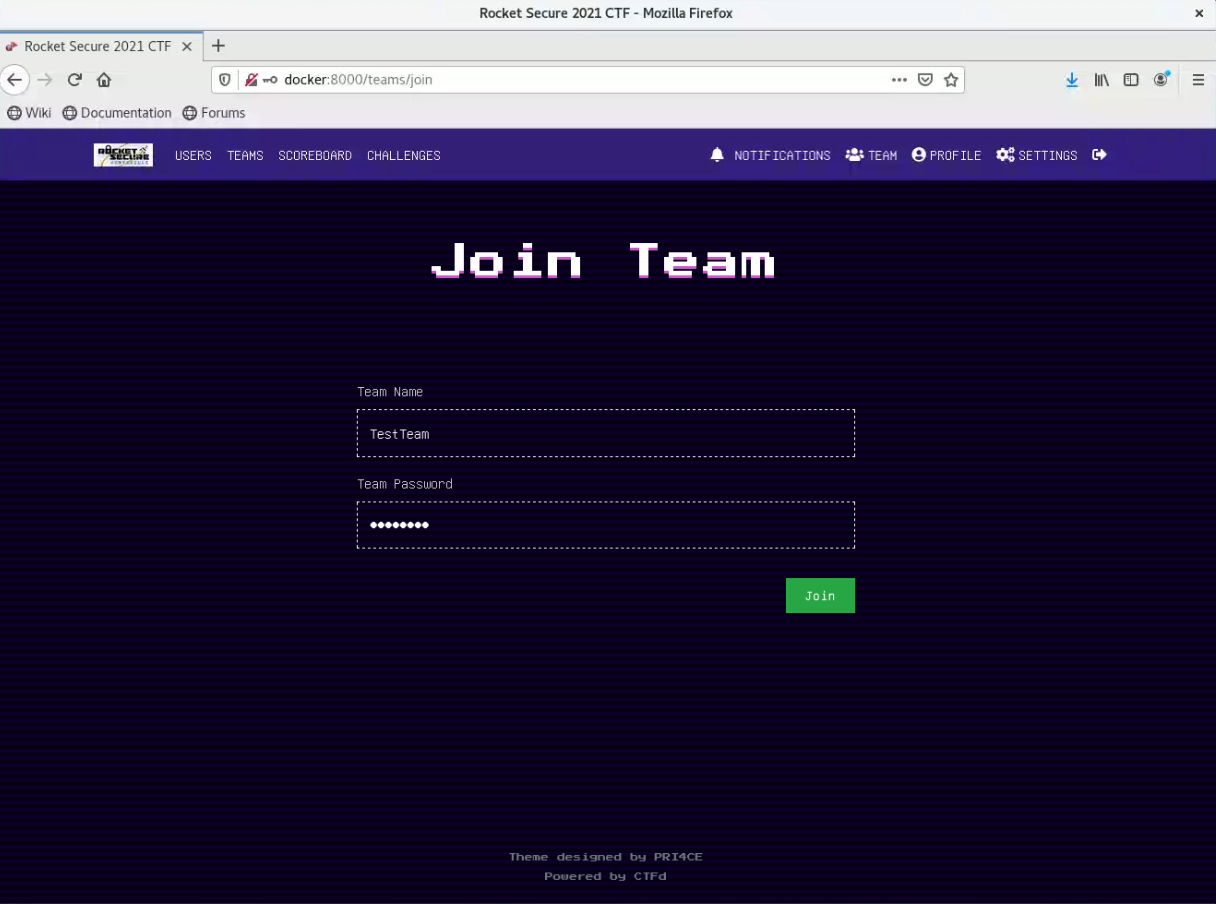
**We ask that you please do not create any team names that include the use of vulgar language or inappropriate references. These challenges are available contestants of all age ranges.**



1. Other users may join your team by selecting the “Join Team” option following the creation of their user account.



1. After clicking “Join Team”, additional team members will be prompted to enter the name of the team they wish to join, as well as the password for that team that was created by the team’s creator or “captain”. After entering the team’s credentials, select the green button labeled “Join”.



1. Once you have created a user account and joined a team, you may begin exploring the different challenge options available to you under the “Challenges” tab.
2. Select the challenge that you would like to attempt first. Each challenge is associated with a different Docker port number, which can be found by clicking on any of the available challenges.

1. **HACK!!!**
2. Finally, use the tools available within Kali and other tricks you have learned along your journey to becoming a hacker and locate challenge flags within each “level” or challenge.
3. Once you locate a flag within your target system, navigate back to the CTF Challenges page (<http://docker:8000/challenges>). Click on the challenge associated with your particular target system and enter your flag value using the following format: **NAC-ISSA{example\_flag\_H@$hValU}**

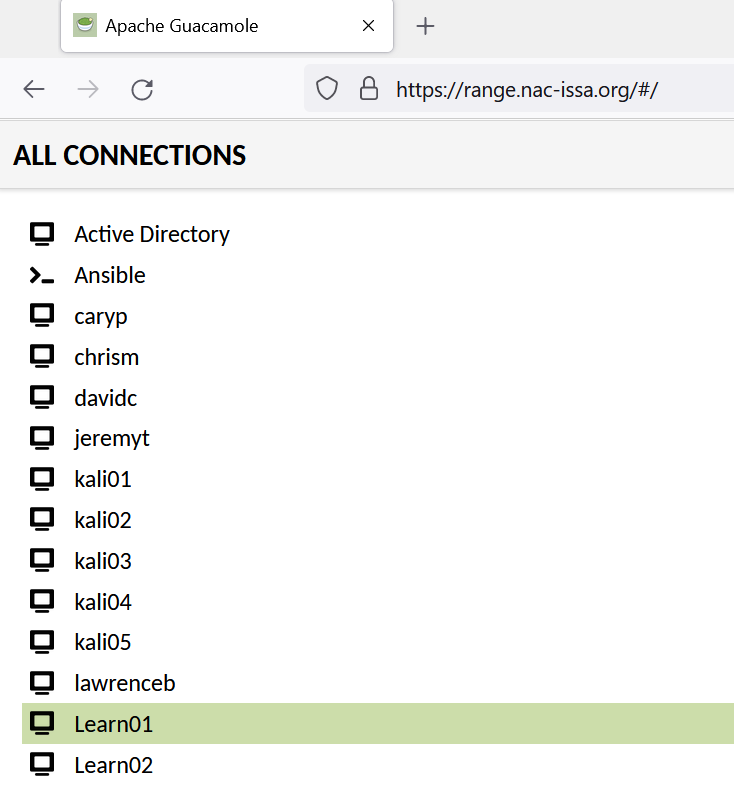
**Note: As more users complete a particular challenge, the score for solving that particular challenge is lessened so that users who solve the challenges first are rewarded with more points.**

## Accessing Student Labs

***Insert Training Intro***

Training activities may be accessed from within the Cyber Range. Please see the login instruction #2 for ***Username***: <your\_username> P***assword***: Password12.

1. Once you are logged into the Cyber Range, hands-on labs may be accessed through any of the “Learn” connections. .



Once inside Lab machines **change directory in the terminal windows** to **~/labtainer/labtainer-student**

From here you may explore the different lab options by simply typing “labtainer”

The system will list approximately 50 labs. Type the full lab name to start the lab, such as “labtainer acl”