Trojan Arena Instructions

Introduction

Welcome to the Trojan Arena where you go head to head with other students in a cybersecurity competition.

Logging into your Computer

On your landing page, you will be provided with a username and password. The username will be cybergym followed by some number, and your password will be a random string of characters. When you are ready, click to enter the arena and log in.

> If your instructor recently started the arena, then it may take up to five minutes for the login screen to show up.

Capture the Flag

Your team will compete for points in the arena. You win points by finding the flags indicated below. For this arena, you do not have to find flags sequentially. In other words, you can work on these as a team in parallel.

Points

Your team will receive points for each of the flags you find. The first team to find a given flag will also receive half of the bonus points. For example, if you find a flag worth 100 points first, then your team receives a total of 150 points. Your team may only submit a flag once.

Submitting Your Flags

The flags will be between two braces or dollar signs. You do not need to copy over the braces and dollar signs. Only copy over the text between them. Once you find a flag, go back to your landing page and type the flag in the assessment section. You can submit any number of times. Once you submit a correct answer, your response will be recorded and timestamped.

To the Arena!

Let’s go! Here are your puzzles to solve. Work as a team, encourage each other, and have fun! Good luck!

Task	Points	Description
1 - Inspection	100	In your browser, navigate to https://cybergym-classified-v7k2apwaqa-uc.a.run.app/inspect and use the inspect tool (Ctrl+Shift+C or right-click inspect) to find the flag You do not need to be in your Cyber Gym Arena for this task. You can click the link above on any computer.
2 - Hidden Weakness	100	We think that there is a user account that shouldn’t be there. Use Nessus to find it. In Firefox, go to https://10.1.0.101:8834. When you go to the site, you will receive a browser warning in Firefox. Click *Advanced* and *Accept risk and continue*. Then login with username: “cybergym” and password: ”Let’s workout!” Create a new basic scan using target 10.1.0.101. On the credentials page click windows and use “cybergym“ and “Let’s workout!“ as username and password.

3 - SQL Injection	100	Our security analysts have reported that they have found a secret UA Little Rock classified database. The only problem…it’s secured behind a login. We don’t know any of the credentials but we do know that they are using a vulnerable SQL database. Perhaps you should try an SQL injection to gain access to the flag? In your browser, navigate to https://cybergym-classified-v7k2apwaqa-uc.a.run.app/sql to start this challenge. Hint: Maybe this article can help us understand what’s going on https://portswigger.net/support/using-sql-injection-to-bypass-authentication You do not need to be in your Cyber Gym Arena for this task. You can click the link above on any computer.
4 - Hidden Site	100	Use zenmap to find the different open ports on a server. To open zenmap, go to Start and type zenmap. In the *Target* box, type in 10.1.0.102, and in the *Profile* drop-down, select *Regular Scan*. Then, in the *nmap output* box, you will find the list of open ports. Open ports allow computers to communicate with each other. For example, if you open a browser and go to https://www.google.com, your computer is using port 443 by default. This is like the main door into the house. However, there are other ways into a computer. For this flag, you will need to find other ports this server may have open. The other ports are like open windows into the house! Then using Firefox, figure out which port leads to the hidden web page and flag. (Ex: http://website.com:###) where ### is some port number.

5 - Password Attack	100	You were hired by a small company to perform a security analysis for one of their physical locations. While doing your normal routine, there is a small building on the far end of the campus that catches your eye. Only one issue keeps you from discovering its secrets – it's PIN protected! Luckily, you've been training your whole life for this moment. On the Windows machine, navigate to the Password Attack folder and open the *Keypad.exe.* Try to guess the PIN. Two key ideas to keep in mind is: • The PIN will be 4 digits long. • No number can be repeated in a PIN.
6 - Steganography	100	Steganography is the practice of hiding text, images, data, or files inside of a different text, image, or data file. For this exercise one of the images on the desktop has a hidden text message. Use the application 'Image Steganography' to decode the image and reveal its secret.

7 - Program Analysis	100	This exercise will test your searching abilities. On the desktop is a document containing some raw data that was captured. Hidden in this data is the flag. You know that the flag is 16 characters long and it is always stored between two curly braces ‘{ }’ and two dollar signs ‘$' such as ‘{$Password$}'. On the desktop is a program called ‘Vim’ that is often found on linux machines. Vim is an open source text editor that was developed long ago in the days before graphical user interfaces were common. Open Vim and then open the file ‘Scramble.txt’ inside of Vim using the menu bar. To search in Vim one needs to simply press the ‘/' key then the characters they wish to search for. For example, to find ‘password’ one would type ‘/password’ then hit enter. One useful concept in many computer tools is wildcarding. You can use wildcards to search for patterns instead of exact phrases. Vim uses the period symbol '.' for wildcards in searches. For example, if you wanted to search for a date where you know the pattern and the year but not the month or day you could search the document by entering ‘/2020/../..’ which would return all results that match the yyyy/mm/dd date pattern from 2020. Now that you are equipped to search large documents find the flag hidden in the Scramble.txt text document.
8 - Arena Snake (Inspect v2)	100	You thought the inspect challenge was too easy, well, now introducing Arena Snake, a not-so-ordinary Snake game. There’s a special flag if you can beat my high score of 100,000! That might take a while since you only get 10 points for each apple eaten. Good luck! In your browser, navigate to https://arena-snake-loader-v7k2apwaqa-uc.a.run.app/arena_snake