


GenCyber Arena Student 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 typically look like this, CyberArena{ d89g0vka4c }. 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.

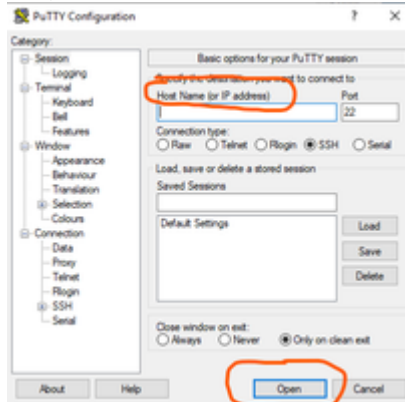
To the Arena!

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 - Crypto	100	<p>Go to the Crypto Challenge under external links. You will be given a ciphertext encrypted using some classical cipher. Using the scenario and hint provided, try to decrypt the message.</p> <p>Note: You can try solving it by hand or write a script to do it for you.</p>
2 - Ransomware	200	<p>One of your clients is under attack and time is quickly running out! Remote into his machine and protect his files before it's too late.</p> <ul style="list-style-type: none"> To connect to the victim's machine, go to the <i>Start</i> menu and search for and click on <i>Remote Desktop Connection</i>. For Computer, use the IP address for the <i>Ransomware</i> machine found on your Cyber Gym landing page. The password is <i>Promiseme!</i> Your goal is to successfully defend the attack before time runs out. If you are able to defend the attack, a flag will appear on the desktop of your Cyber Arena machine. <div>  Be careful not to close any windows in the Ransomware machine as this could prevent the flag from appearing. </div>
3 - IoT	200	<p>Click on the link on your landing page to enter the IoT portion of the arena, and enter your device ID at the prompt. Then investigate the page (similar to the IoT workout earlier in the week), and use the information you find to reveal the flag.</p> <div>  Hint: the device itself will give you valuable information. Pay close attention to the LEDs </div>
	200	

4 - Social Engineering

On your Cyber Arena machine, use the PuTTY application on your desktop. For the Host Name, type the IP address of the Kali server shown on your landing page (e.g. 10.1.x.y). Then click *Open*



Use the credentials:

Username: kali

Password: P@55w0rd!

Once in Kali, you will be using the tool Social Engineering Toolkit provided as open-source by TrustedSec and authored by David Kennedy. Follow these instructions to mount the attack:

		<ol style="list-style-type: none"> 1. To use the tool type <code>sudo setoolkit</code> at the command line and retype the password from above. 2. The tool will prompt you to agree to the terms of use. If you agree, type <code>y</code> to continue. Then a menu will pop up with various attack modules. 3. Select 1) Social Engineering Attacks 4. For the type of attack to mount, select 2) Website Attack Vectors 5. Next, select 3) Credential Harvester Attack Method. 6. Then, you will be provided options for generating the fake website. Choose the first method, which pulls predefined web templates: 1) Web Templates 7. The tool will take a few seconds to prepare, and then it will ask you the IP address of the attacker machine. Type in the IP address of the Kali server (same as above from the landing page). 8. Finally, you will be provided with a template for the fake website. Use 2. Google. <p>Give it a few minutes, and you should start seeing credentials coming in with the flag. You will also be given some special instructions to deduct points from your opponents.</p>
6. Open Source Intelligence	100	<p>A client needs help finding a location. The only information you have is the picture provided.</p> <p>On the desktop of your Cyber Arena machine, open the image <code>so_mysterious</code> and use your Googling skills to see if you can figure out what building on the right in the picture is.</p> <p>The flag is the name of the building on the right.</p>

7. Hack The Shapes	100	<p>On your desktop is a folder called HackTheShapes that contains a game. There is a flag at the end of the game, however the game is very difficult. To make the game easier we have installed Cheat Engine, located on your desktop, to use to help you get to the flag.</p> <p>Controls</p> <p>Arrow Keys Movement</p> <p>Z Drop Money</p> <p>Enter Interact with NPC or Info</p> <p>Hold Shift Run</p> <p>Hold Ctrl Slow walk</p> <p>R Restart game</p>
8. Denial of Service	100	<p>On your workout home page there is a server called <i>web-target</i> that has a seal on it. Somewhere on their end is a hidden flag that is revealed when they have a lot of traffic on their site. Use LOIC located on your desktop to do so, using the IP for your web-target for the IP, and change the attack method to HTTP. Finalize the attack using the button labeled <i>IMMA CHARGIN MAH LAZER</i>.</p>