Trojan Arena Level 1 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.

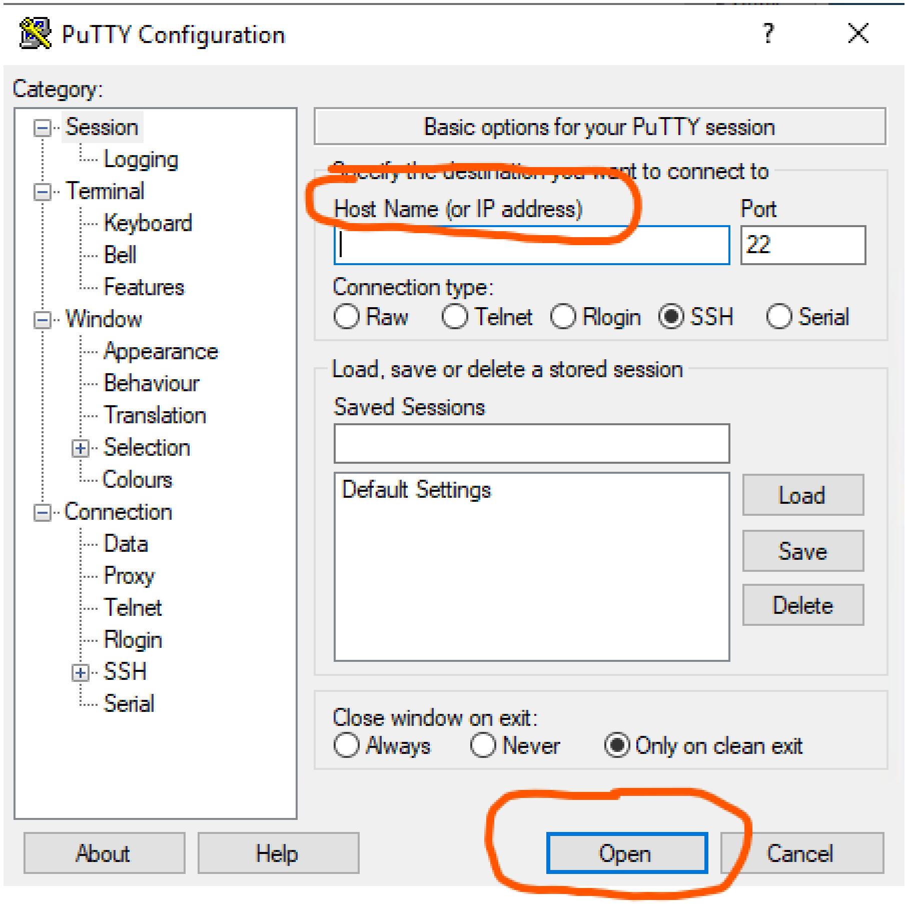
Submitting Your Flags

The flags will typically look like this, Cybergym{ 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 - Open Source Intelligence	100	A client needs help finding a location. The only information you have is the two pictures provided. On the desktop of your Cyber Gym machine, open the folder called *OSINT* and use the two images and your Googling skills to see if you can figure out what building is shown in the picture. The flag is the full name of the building.
2 - HumptyDumpty	100	We found a QR code that seems to be broken. Can you fix it? On the desktop of your Cyber Gym machine, look for the file called *HumptyDumpty.psd* and open it with *GNU GIMP* and see if you can put Humpty Dumpty back together again.
3 - Forensics	100	Log into the MobileForensics server by opening a Remote Desktop Connection on your server. For the Computer, use the IP address shown on your landing page for *Forensics* (e.g. 10.1.x.y). Then use the credentials: **Username:** *forensics* **Password:** I swear 2… In the Tools folder on the Desktop, open the *Autopsy* tool. Click to open a recent case, and select *George Cell Phone*. Give this a few minutes to load the mobile phone image. What almost ate the monkeys on Christmas Day?
4 - Space Gifs	100	For some reason our space team has decided to communicate only in gifs. Can you figure out what they’re trying to tell us? On the desktop of your Cyber Gym machine, look for a file called rocket.gif and see if you can find the secret message.
	100	

5 - Social Engineering		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*  PuTTY Configuration ? × Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial Basic options for your PuTTY session Load Save Delete About Help Open Cancel Specify the destination you want to connect to Host Name (or IP address): Port: 22 Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial Load, save or delete a stored session Saved Sessions: Default Settings Close window on exit: ○ Always ○ Never ● Only on clean exit 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:

		1. To use the tool type `sudo setoolkit` 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 *y* 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`. 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.