Container Security: What Could Possibly Go Wrong? Practical Part

Two things are needed to participate in the practical part of the session:

- KYPO platform to access the game environment
- SSH access to interact with the prepared virtual machines

KYPO platform

This platform will guide you through the game environment itself. It contains game levels, descriptions of the tasks and hints to finish the tasks. To pass to the next level, you will always need to submit the flag specified in the description.

1. Book your account at: <u>https://docs.google.com/spreadsheets/d/1gs2DPeYRO1gAdQS78D721GX5BAIrIG</u> <u>WUKciKT1ua6Y/</u>

Just pick up a free line and put your name there (or other identifier of yours).

2. Go to <u>https://isgc.crp.kypo.muni.cz</u> and login with the booked credentials.

🔬 κύρο		2
A KIPO	Home	
	Login with On your first login you will be registered with OIDC provider. If you are already	
	registered select your provider.	
	Login with local issuer	
	Access consent When accessing the KYPO Cyber Range Platform, your personal data, such as	
	your name and e-mail, as well as any data generated by your interaction with the KPPO Cyber Range Flatform, will be processed for the purposes of the	
	providing the service and only for this period to ensure proper operation of the service. After the termination of the service, your personal data will be	
	anonymized and further used only for scientific and research purposes. This will apply as well to other data created by your interaction with the KYPO Cyber	
	Range Platform. For more information, please contact us at info@kypo.cz.	

3. You will get into an intro page of Training Runs.

KYPO Home / Training Runs Infrest Training Run Overview Infrest Access Training Fill in access token provided by the organizer to start the training. Access Token Prefix * - Access Token PIN * Infrest Access Token Prefix * - Access Token PIN *	
m Training Run Overview Access Training Fill in access token provided by the organizer to start the training Access Token Prefix* Access Token Prefix* Access Token PIN*	
Access Training Fill in access token provided by the organizer to start the training Access Token Prefix * Access Token Prefix * Access Token Pill *	
Fill in access token provided by the organizer to start the training Access Token Prefix * - Access Token PIN *	
Access	
	_
Title Date Completed Levels Actions	
Docker Security training 21 Mar 2021 16:24 - 26 Mar 2021 00:00 1/16 🚺 🔝	

4. You will be able to start the *Docker Security training* by clicking on the button **Resume training run**.

No Access Token needed!

🚯 күро						۵	(
C KIPU	Home / Training Runs	;					
Trainings							
Run			Training Run Overv	iew			
			Access Training Fill in access token provided by the organizer to s	tart the training			
			Access Token Prefix * A	ccess Token PIN *			
				Access			
		Title	Date	Completed Levels	Actions		
		Docker Security training	21 Mar 2021 16:24 - 26 Mar 2021 00:00	1/16	1		
				Items per page: 10 💌	1-1of1 < < > >		

5. After clicking on the button **Resume training run**, you will get to the first page of the game.



6. Wait for the **first flag to be given to you** during the presentation.

SSH access

There are two possible ways to interact with the prepared virtual machines:

- directly using SSH
- embedded console

Directly using SSH via the Internet

Please, see the topology shown in the presentation.

DO NOT use the Get SSH Access button inside the KYPO platform.

Embedded console inside the KYPO platform

You may use an embedded console inside the KYPO platform. Nevertheless, we recommend you to use direct SSH access.

After clicking Next....

😥 κύρο		🌲 😁 ~	
A KTPO	Home / Training Runs / Game		
Trainings			
Run		User1	
	0 — • — • — • — • — • — • — • — • — • —	user1	
		00:00:02	
	Docker Security Training		
	Welcome to this short Docker Security Training. There is a short introductory part and then three tasks which will illustrate common misconceptions regarding Docker.		
	Each task is divided into several levels to provide you with smooth passage through the training. There is a description of your task at each level and also the description of the flag you need to submit to get to the next level. If you want, you can have hints revealed to you how to finish the task. In case you have no idea what to do, you can have the whole solution revealed. Beware of the fact that you cannot go back to any of the previous levels.		
	In case you are stuck, we encourage you to search a bit on the Internet or check the information in the introduction. Have fun!		
		Next	

You will see the topology below.

Sandboxes Definition	Start of the game		
Pool	Please wait till we tell you the flag to start this training session :)		
Resources	=	Solution Flag Submit	
Administration	route-ne	Solution Flag Submit	
User		Get SSH Access	
Group			
Microservice			
	() 100.100.1 router		
	training		

To get to the embedded console, double-click on the training. 10.20.30.100 main will appear.



Click on the 10.20.30.100 main with the right button. Several options will appear.



Click with the left button on the Generate console URL option and wait a few seconds till the option Open console appears.



After clicking on the option Open console, a new window will be opened with the embedded console.

SPICE	
Ubuntu 20.04 LTS main tty1	
main login: _	
Send Ctrl-Alt-Delete	