

Hands-on Part

CyberRange^{cz}

Powered by CyberRange^{cz} Platform

- **Open-source** platform built on real security exercise experience.
- **Sophisticated** cloud infrastructure delivers realistic training environments.
- **Hands-on** security training with integrated monitoring and analysis.

cyberrange.cz

Environment

- Book an instance at <https://go.egi.eu/tcscs2025>
 - Pick up a free line and put your name there (or another identifier)
- SSH access
 - `ssh -p PORT training@147.251.88.203`
 - **PORT** is available from the sheet with booked credentials
 - Password:
- Register account at <https://tasks.metacentrum.cz/> and start
 - Registration code: **tcsc-25**

Summary of the tasks

Tasks

- Privilege escalation
 - Using a container to access information not visible to the user
- Remote try
 - Unsecured Docker daemon provides a full access to the system
 - Either crafting API calls or using a Docker client
- Escaping from containers
 - Manipulating cgroup to start a process outside the container

Summary

- Privilege escalation
 - A ordinary user can start process as root, and can get access to any resources
 - Access to Docker daemon provides full access to the system (local or remote)
- Container escape
 - Isolation can be fragile and depends on container setting
 - Possibility to make use of “common” tools (hooks, filesystem access)

Conclusions

- Pay attention to proper configuration of **containers and their privileges**
- Make sure access to Docker daemon is granted only to **trusted users**
- If Docker daemon is available over network, it is **properly secured**
- Consider enabling **user namespaces**
- Consider other approaches, such as **root-less container technology** (singularity, podman)