How to design your hands-on cybersecurity training in KYPO CRP

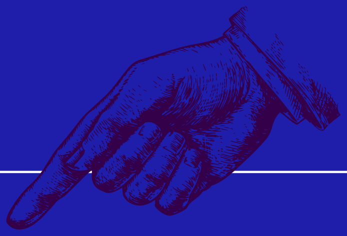
FIELD MANUAL

v1.0

The need for skilled cybersecurity staff has never been higher.

You know it.
We know it.

Hands-on training is part of the solution.



This manual is a good start.

What do we understand as cybersecurity hands-on training?

» **Hands-on for red or blue team**

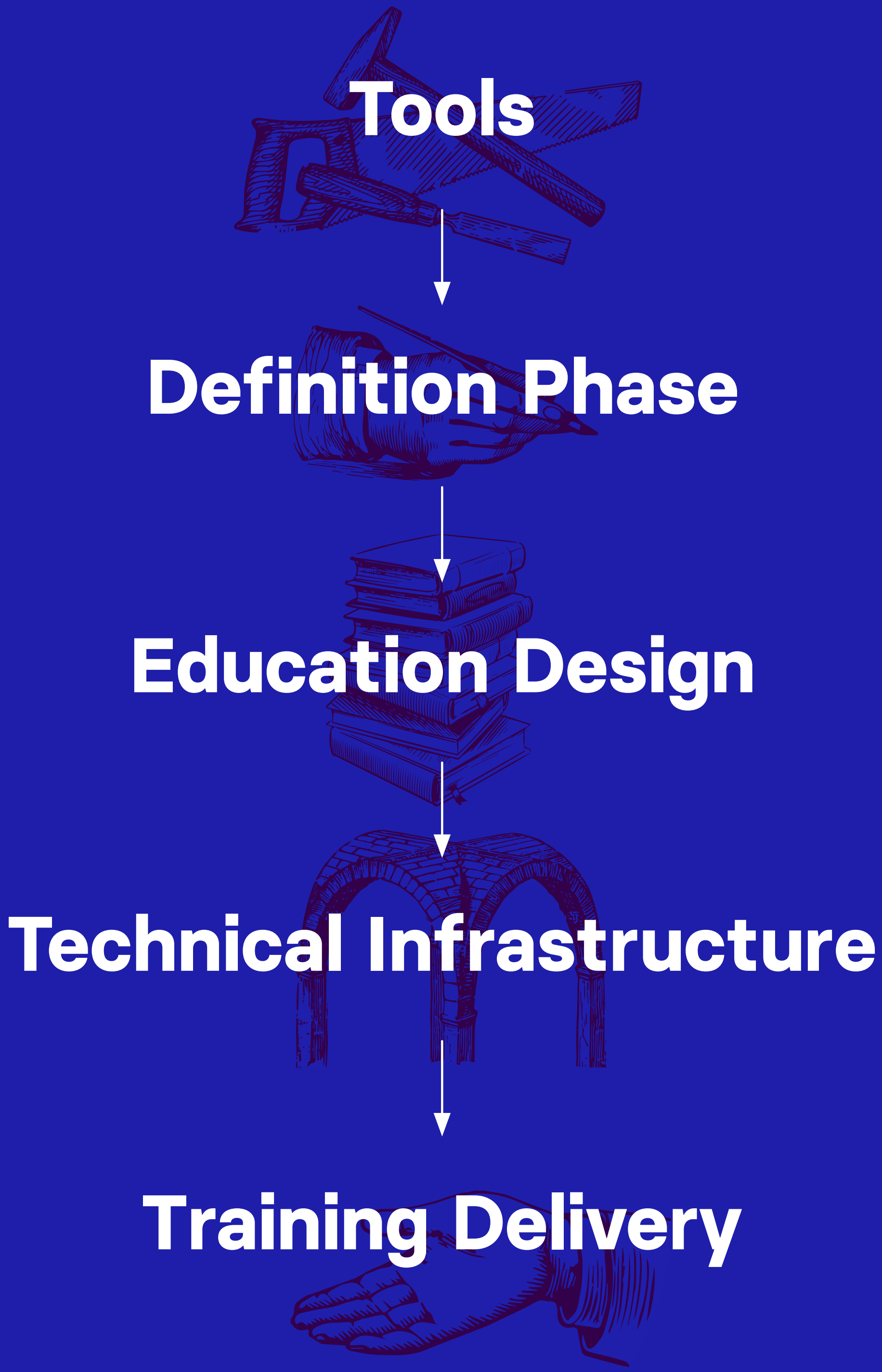
» **Level-based structured learning**

» **Monitoring and feedback tools**

» **In the class or remote learning**

» **Easy to design and develop**

How do we design it?



Tools

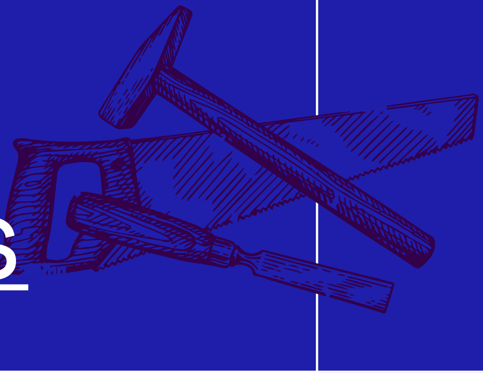
Definition Phase

Education Design

Technical Infrastructure

Training Delivery

Explore your tools



Your training design process starts with the selection of proper tools. We offer you two open-source technologies. Fully-fledged Cyber Range or its lite version that can be deployed really simply.

KYPO CRP

- First open-source cyber range in the EU
- Developed since 2013
- Built on top of the OpenStack cloud
- Proven in practice
- Open-source under the MIT license

https://gitlab.ics.muni.cz/muni-kypo-crp

KYPO CRP LITE

- Can be deployed with zero configuration
- 4 commands and 40 minutes to have your KYPO CRP
- Allows to evaluate KYPO CRP or create KYPO training without being a DevOps expert.
- Can be deployed to the most major cloud providers, or powerful desktop/server
- Cannot host training for more participants

https://gitlab.ics.muni.cz/muni-kypo-crp/devops/kypo-lite

Define fundamentals

Set your goal and ideate the scenario.

1. Goal setting

What are the goals?

- Example: *Demonstrate to students how to get root on the machine*

Is it the Red team or the Blue team scenario?

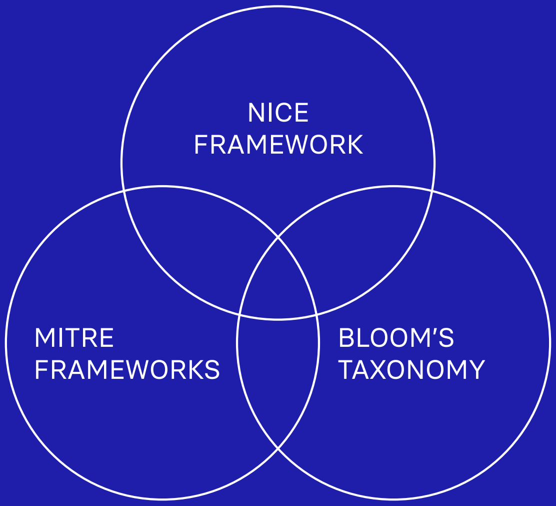
- Example: *Red team*

Who is the target group?

- Example: *Students with minimal previous knowledge*

Structure and length?

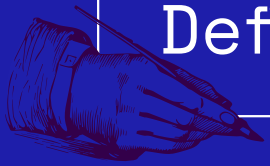
- Example: *Class-based, circa 2 hours*



Maximize the impact of your training

Conduct needs analysis and map your findings to:

- NICE Framework (work roles)
- MITRE Frameworks (adversarial tactics and techniques)
- Bloom's taxonomy (learning objectives).



Define fundamentals

2. Scenario ideation

What is the story?

- Example: *You are junior penetration testers with a task to assess the company’s server*

What is the real-life example?

- Example: *Explain to students how penetration testers work, including tools and write-ups*

What are the goals (more details)?

- Example: *Train ability to identify security issues based on the analysis of vulnerability and configuration data (A0001) – based on the NICE Framework*

Example:
Use Reconnaissance (TA0043), Initial Access (TA0001), and Privilege Escalation (TA0004) – based on the MITRE Frameworks

Focus on learning design

Create a training definition and optimize the learning experience.

1. Training Approach Selection

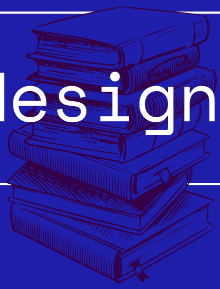
Think about your goals and scenario that you defined and select your approach.

» **Defense Oriented** – To study and practice the defense methods.

» **Attack Oriented** – For deep understanding of the attack methodologies to know how to efficiently mitigate them.

» **Mixed** – Combines the defensive approach with the offensive approach and is the most comprehensive method.

Focus on learning design



2. Preparation of Tasks and Rules

Write catchy and understandable assignments based on learning objectives and selected approach.

» Create answers and step-by-step solutions.

» Create hints to help players complete selected tasks.

» Set clear and fair rules, including anti-cheating policies.

» Approach *„whatever is not explicitly prohibited is permitted“* is best.

3. Gamification

It is highly recommended to use gamification to support players’ engagement.

Gamification Elements:

» **Narrative**
Background story, which should gradually provide players more necessary information.

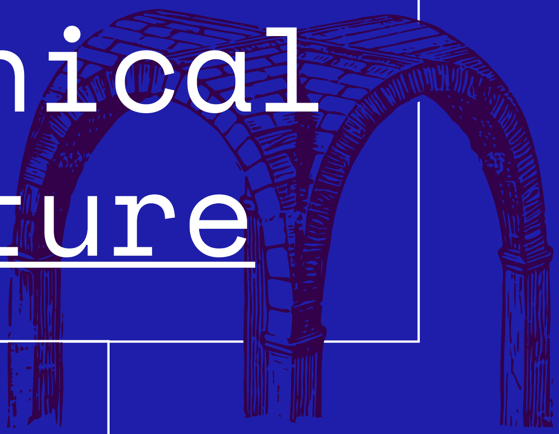
» **Injects**
Simulated events in the game to enhance learning goals.

» **Players‘ Identity**
Players can feel like their game character.

» **Rewards**
Represent added value to the evaluation of the player’s performance.

Build technical infrastructure

Prepare a virtual training environment.



1. The match with your scenario

This is a necessary part at the beginning, for an example: *Think about what you need to prepare at the beginning of this phase.* The environment must be created for the training scenario.

Your thinking might look like this: *We need a simple network with a Kali machine and a Vulnerable machine for this training.*

Kali machine

- Add our dictionary for Hydra

Vulnerable machine

- Locate telnet on nonstandard port
- Set telnet password from the dictionary
- Prepare misconfiguration to escalate privileges

Once you specify what you need for training you can move to preparations. The whole process is pretty straightforward and well structured.

2. Virtual machine images in OpenStack

Start with the preparation of images in OpenStack. The process consists of 3 steps:

Download images:

- Images created by us
  https://object-store.cloud.muni.cz/swift/v1/kypo-images/
- Official cloud images
  https://docs.crp.kypo.muni.cz/installation-guide/openstack-requirements/#images

Develop images manually:

- Repositories of our images
  https://gitlab.ics.muni.cz/muni-kypo-images
- Guide for developing an image
  https://gitlab.ics.muni.cz/muni-kypo-images/muni-kypo-images-wiki

Import images into OpenStack:

- Guide for importing an image
  https://gitlab.ics.muni.cz/muni-kypo-images/muni-kypo-images-wiki/-/wikis/How-to-upload-an-image-to-OpenStack

3. Sandbox definition

Now you need to create sandbox definitions. That means how the topology and its configuration will look like.

Create topology definition:

» Define Hosts, Routers, Networks, Groups, *Net/router_mappings*) in *topology.yml* file.

See the example of sandbox definition

Prepare Ansible roles:

» Configure the machines with services by using Ansible roles.
» You can develop your own or download roles created by the community galaxy.ansible.com.

Check the example of ansible roles

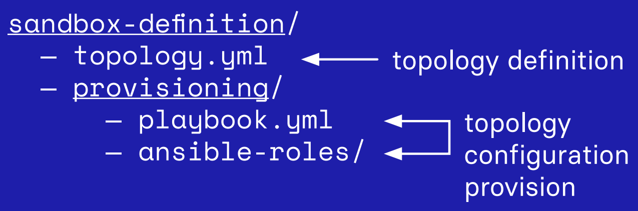
Create Ansible playbook:

» Finally, map the roles to hosts that you created in *toplogy.yml*.

See the example of ansible playbook

What is a sandbox definition?

It consists of two parts. The first one is topology definition (.yml) and the second part describes topology configuration provision.



```
sandbox-definition/
  – topology.yml
  – provisioning/
      – playbook.yml
      – ansible-roles/
```

topology definition

topology configuration provision

Ansible in a nutshell

» Agentless configuration management software
» Administrators tell the software what should be done but not how

Ansible uses:

» **modules** to accomplish a given task (e.g. apt module for installing a software package)
» **tasks** to call an Ansible module
» **roles** to group and encapsulate Ansible artifacts (e.g. tasks, variables, files...)
» **plays** to map roles to hosts

Build technical infrastructure

4. Building sandbox

This is the final part where you will build a sandbox in the KYPO Cyber Range Platform. It consists of two steps.

First, you will import the sandbox definition,

and second, you will create and allocate pools. We have guides for both of these processes.

Guide for importing sandbox definition

Guide for creating and allocating pool

Deliver the training

Prepare smooth and nice experience for your training participants. You can use this checklist:

- □ **Prepare intro information and study materials**
- □ **Explain how the KYPO CRP works**
- □ **Have a technical support ready.**
- □ **Write notes during the training.**
- □ **Gather feedback.**
- □ **Write down lesson learned.**

Next steps

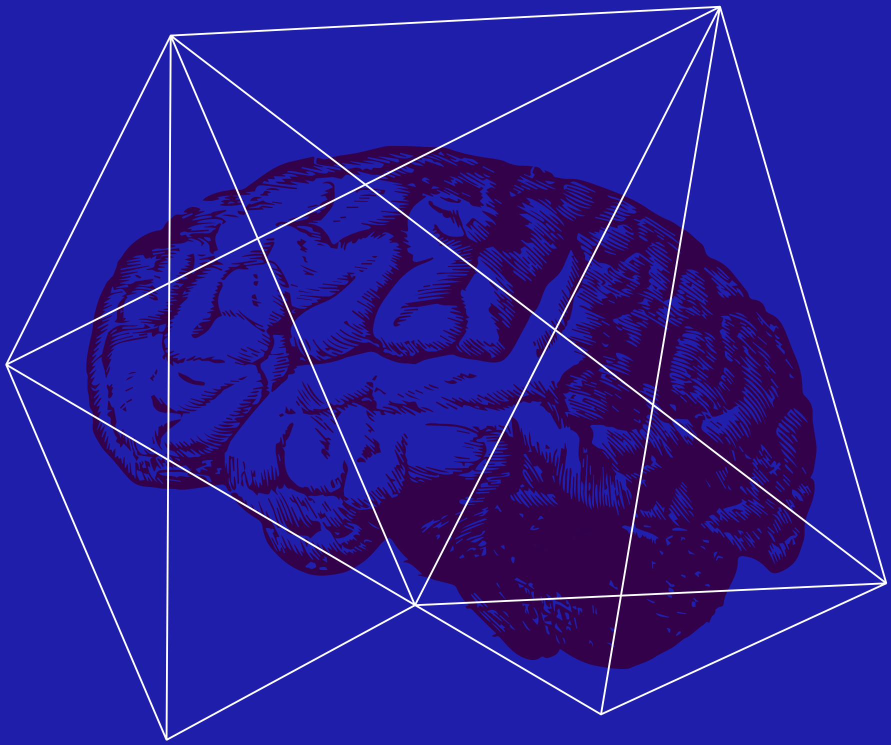
Check our website. It is the main entry point to everything you need to know
(*including the documentation*)
kypo.cz

Follow us on Twitter!
twitter.com/KYPOCRP

Join our LinkedIn group
Cybersecurity exercise & training designers
muni.cz/go/kypodesigners

Learn about the KYPO services we offer
kyposervices.cz

Contact us if you are interested in cooperation
info@kypo.cz



Supported by Concordia H2020

CONCORDIA is operating a pilot for a Cybersecurity Competence Network. Its consortium consists of 56 partners (universities, industries, and public bodies). CONCORDIA is a part of a significant European-wide effort to boost the EU's digital sovereignty.

CONCORDIA project has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927.

www.concordia-h2020.eu