MUNI FI

Scalable Learning Environments for Teaching Cybersecurity Hands-on

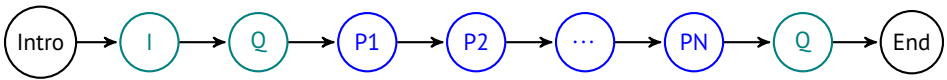
Jan Vykopal, Pavel Čeleda, Pavel Šeda, Valdemar Švábenský, Daniel Tovarňák
vykopal@fi.muni.cz

Masaryk University, Czech Republic

October 2021 @ FIE'21 conference

Cybersecurity Hands-on Classes

- Learners **interact with networks** of full-fledged operating systems and devices that **emulate real-world systems**.
- Learners' interaction is **driven by a learning environment** with or without a human instructor's assistance.
- Each student or team works with an **own instance** of the lab environment.



Generic structure of training with several phases (P),
optional questionnaires (Q), and informative phases (I).

Problem Statement

Cybersecurity hands-on classes do not scale.

- Preparation requires a substantial effort.
- Delivery issues in large classes.
- Providing feedback and analyzing learning gains is difficult.

Goal of the Paper

Enable scalable teaching of cybersecurity hands-on classes using interactive learning environments.

Building Blocks of a Cybersecurity Hands-on Class

- **Sandbox** – an isolated environment for practicing cybersecurity skills.
- **Class Delivery Method** – a computer-assisted instruction that employs the sandbox.
- **Learning Analytics** – components analyzing students' interactions in the sandbox and the class delivery.

Building Blocks – Scalable Approach I

Sandbox Definition = **Topology Definition** + **Provisioning Definition**

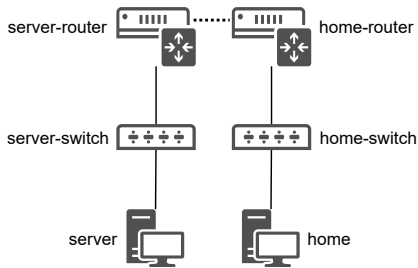
- Structure of the networks and hosts and their configuration.
- Topology definition of a sandbox in YAML.

```yaml
networks:
  - name: server-switch
    cidr: 10.10.20.0/24

  - name: home-switch
    cidr: 10.10.30.0/24

net_mappings:
    - host: server
      network: server-switch
      ip: 10.10.20.5

    - host: home
      network: home-switch
      ip: 10.10.30.5
```



Building Blocks – Scalable Approach II

Provisioning Definition – configuration changes at the hosts in the topology definition.

- Used to customize the **base boxes** – a minimal installation of a particular OS.
- Specifies applications and data that have to be provisioned at the base boxes.
- Input for **software configuration management system**; we use Ansible.
- More flexibility in preparing the sandbox – **reuse** of the definitions for other classes.

Building Blocks – Scalable Approach III

- **Example of a provisioning definition** with two tasks installing a web server and provisioning files of a web application at the host named `server`.

```
- hosts: server
  become: true
  tasks:
    - name: Install Apache, MySQL and PHP5
      apt:
        name: [apache2, mysql-server,
               php5-mysql, php5]
        state: present
        update_cache: yes

    - name: Copy app to the web root
      copy:
        src: web-app/
        dest: /var/www/html
...
```

Building Blocks – Scalable Approach IV

Training Definition – machine-readable description of consecutive tasks that have to be solved by each student.

Example of one training phase with two hints in a JSON format:

```
{
"title": "Looking for a vulnerable service.",
"max_score": 100,
"level_type": "TRAINING",
"order": 1,
"estimated_duration": 5,
"flag": "service-name-1.23",
"content": "Now you need to scan the server to find
   possible vulnerabilities. The IP address of
   the server is **10.1.26.9**. The name of the
   vulnerable service starts with \"s\". \n\n
   As a flag, submit the name of the vulnerable
   service in the following format: _service-version_.
   All characters are lowercase. For example:
   _dvwa-2.050_.",
"solution": "```root@attacker:~# nmap -sV
   -p 10000 10.1.26.9\n```\n\n
   The flag is: **service-name-1.23**",
"hints": [ {
"title": "Which port should you scan?",
"content": "The vulnerable service is running on
   port 10000. You can also pass this information
   to nmap (**-p \"port range\"**).",
"hint_penalty": 10,
"order": 1
},
{
"title": "Which  tool should you use?",
"content": "You should use **nmap** to scan the
   server (see **man nmap**).",
"hint_penalty": 10,
"order": 0
} ],
"incorrect_flag_limit": 100,
```

Building Blocks – Scalable Approach V

Learning Analytics Stack – a mechanism of processing **events** from the environment.

- Events capture **interactions of the student** with the environment: sandbox and class delivery method (training).
- Events are machine-readable strings logged using the **Syslog protocol** (RFC 5424) in a predefined format.
- The learning environment forwards all events to the **central storage**, which transforms and further processes them.
- The central storage uses the **ELK stack** – Elasticsearch, Logstash, and Kibana.

Building Blocks – Scalable Approach VI

Command **ssh alice@server** executed by a student in the Linux terminal at a machine in the sandbox, timestamped and logged into Syslog.


```
{
  "timestamp": "2021-02-17T09:17:33+02:00",
  "username": "root",
  "hostname": "client",
  "host_ip": "10.10.40.5",
  "wd": "/home",
  "cmd": "ssh alice@server",
  "cmd_type": "bash-command",
  "sandbox_id": "1"
}
```


More details in the following paper:

`https://www.muni.cz/en/research/publications/1783801`

An event of submission of an **incorrect answer .invoices2019** to a task in a training phase.

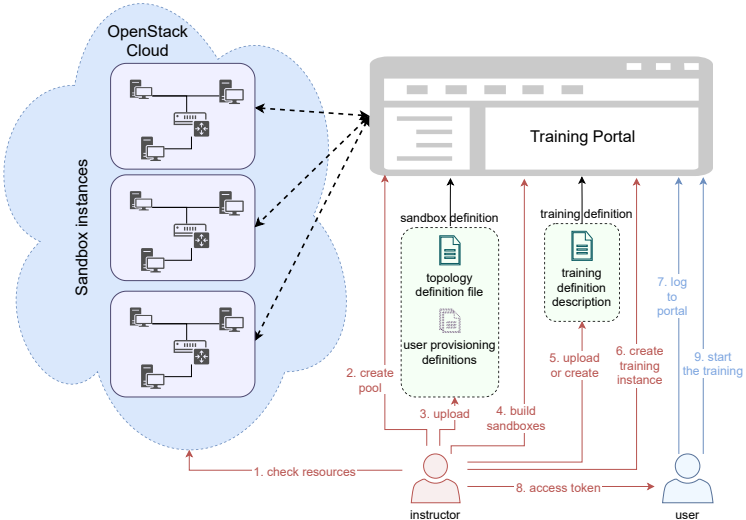

```
{
  "flag_content": ".invoices2019",
  "actual_score_in_level": 100,
  "total_score": 300,
  "game_time": 3045985,
  "timestamp": 1610618680221,
  "type": "events.trainings.WrongFlagSubmitted",
  "count": 1,
  "user_ref_id": 19,
  "phase_id": 36,
  "training_run_id": 28,
  "training_instance_id": 12,
  "training_definition_id": 7,
  "sandbox_id": 104,
  "pool_id": 40
}
```

Learning Environments

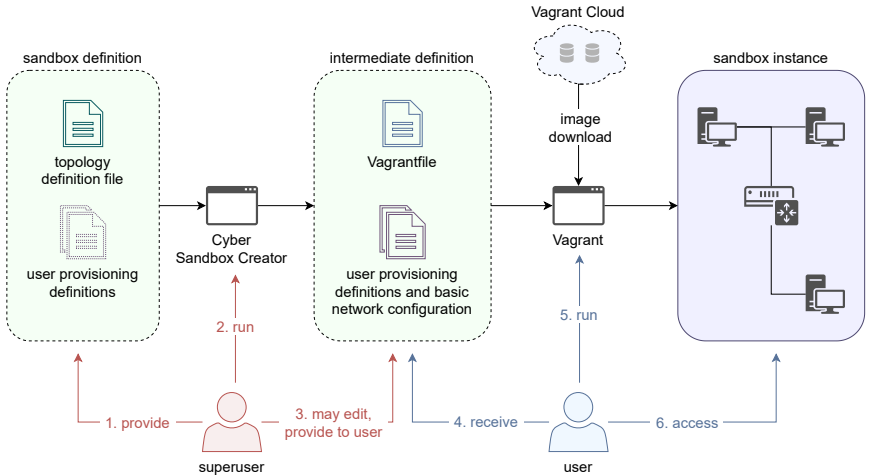
Based on the common components, we developed two learning environments:

- **KYPO Cyber Range Platform** (KYPO CRP) – a cloud-based platform for running multiple classes in parallel or classes requiring sandboxes with many hosts.
- **Cyber Sandbox Creator** (CSC) – lightweight, distributed lab environment using a computer in a school lab or students' own desktop or laptop.
- Both environments use the **same formats** for topology, provisioning, and training definitions, and the same formats of events processed by learning analytics stack.
- Instructors can **choose** the environment that better suits their needs.

KYPO Cyber Range Platform Architecture



Cyber Sandbox Creator Architecture



Use Case – Formative Assessment in Large Classes

- Students gain hands-on experience with using various cybersecurity tools.
- Using CSC, everyone can **deploy the sandbox locally** on their own computer.
- CSC is suitable in **low-stakes contexts** (students can see the sandbox definition).
- Local deployment does **not need any cloud resources** (unlike KYPO CRP).
- Teachers need to prepare **detailed setup instructions**, as well as be ready to troubleshoot the setup.

Use Case – Summative Assessment

- In summative assessment (final exam, competition), we need to **hide the sandbox definitions** from students.
- KYPO CRP provides access to the **sandbox deployed in a cloud**.
- Students connect to the machines in the sandbox, but **cannot see their definitions**.
- Teachers can **control the visibility of hosts** in the sandbox topology (students initially start at one machine).

Conclusions

- We provide **scalable and reusable building blocks** for cybersecurity hands-on classes.
- We exploit these blocks for developing **two learning environments**:
  - **KYPO Cyber Range Platform** – cloud-based → OpenStack,
  - **Cyber Sandbox Creator** – host-based → VirtualBox.
- Open definitions of formats enable educators to **enhance and edit** the existing lab environments **without much additional effort**.
- The environments have been used in **teaching at multiple institutions** since 2019.
- Both environments have been **released as open-source software**.

Publicly Available Contributions

KYPO Cyber Range Platform source code
https://gitlab.ics.muni.cz/muni-kypo-crp

KYPO Cyber Range Platform documentation
https://docs.crp.kypo.muni.cz

Cyber Sandbox Creator source code
https://gitlab.ics.muni.cz/muni-kypo-csc/cyber-sandbox-creator

Full paper and slides
https://www.muni.cz/en/research/publications/1783808

Stay in Touch

Jan Vykopal
vykopal@fi.muni.cz

MUNI KYPO Portal
https://kypo.muni.cz

KYPO Cyber Range Platform
https://twitter.com/KYPOCRP

Cybersecurity Laboratory
https://twitter.com/cybersecmuni

MUNI
FACULTY
OF INFORMATICS