moodlemoot

Virtual Cyber Exercises with Moodle

Adam Welle and Kimo Bumanglag
Carnegie Mellon University

Legal slide

Agenda

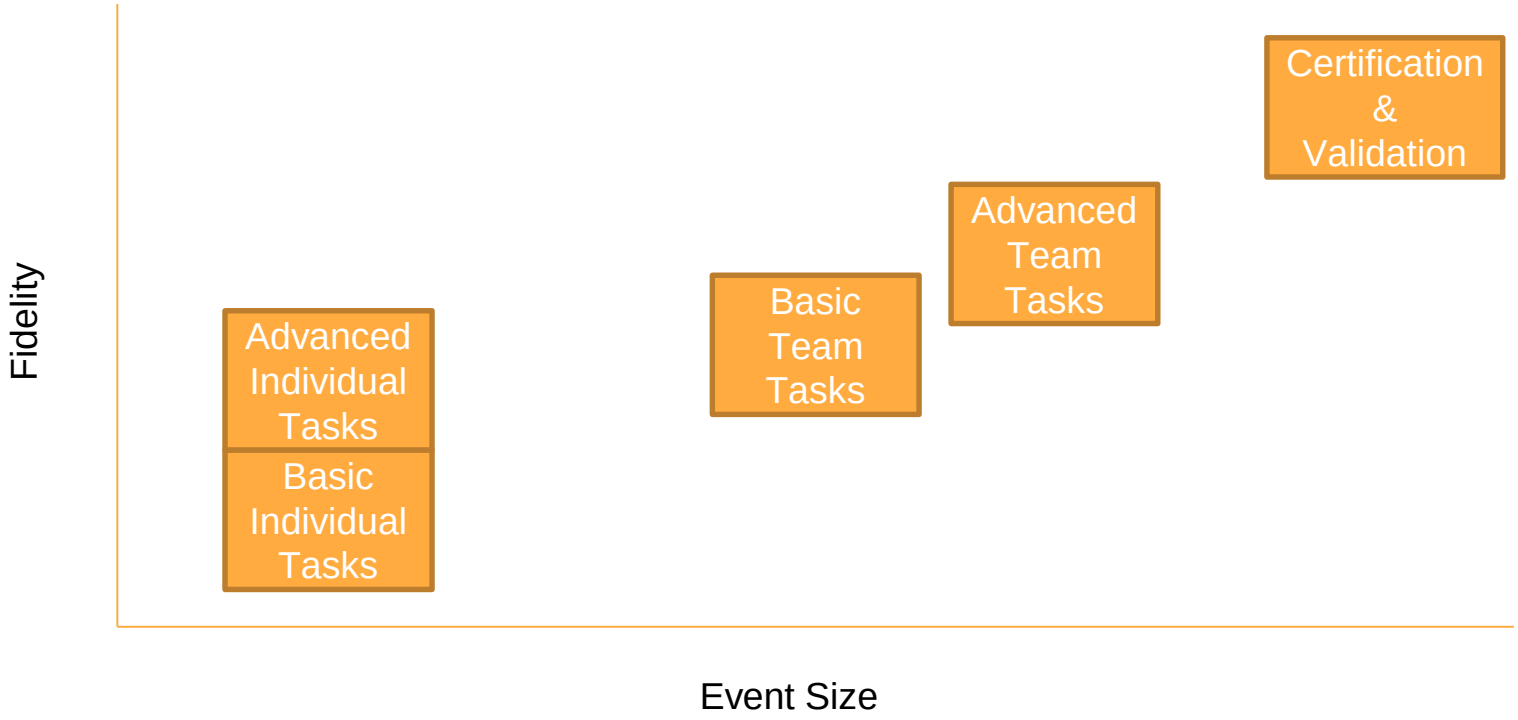
- Introduction
- Cyber Exercise Overview
- Training Objectives
- Range Technologies
- Simulations
- Integrating with Moodle

Introduction

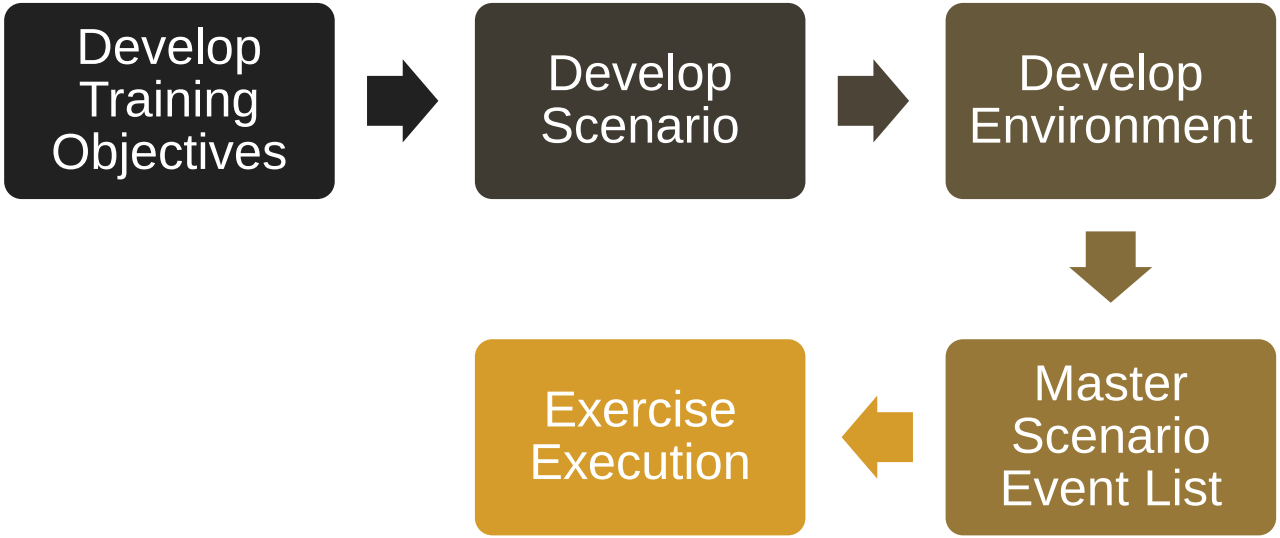
- Who we are
- What we do

moodlemoot

Cyber Exercise Overview



Training Objectives



Range Technologies

Deprecating

Open Source Lab Builder

Full Scale Environment Builder

Coming soon

Simulations

- GHOSTS
  - for Non-Player Characters
- GreyBox
  - for backbone routing
- TopGen
  - for Simulated Internet websites and DNS
- vTunnel
  - for out of band command and control
- WELLE-D
  - for Wi-Fi simulation
- StormBox
  - for low fidelity user simulation

Integrating with Moodle

Activities & Plugins

- Quiz
- H5P
- VPL
- Course Format Board
- Logstore XAPI
- Local Metadata

Assessment

- LMS – Moodle, of course!
- xAPI – from Moodle, H5P, and VMs
- MELK – Moodle, Elasticsearch, Logstash, Kibana to visualize performance
- Cyber Evaluator Tool – Competencies

Moodle Development

- Content Sync
- Course import from old STEP LMS
- Crucible VM console access
- Custom Theme

Moodle Development

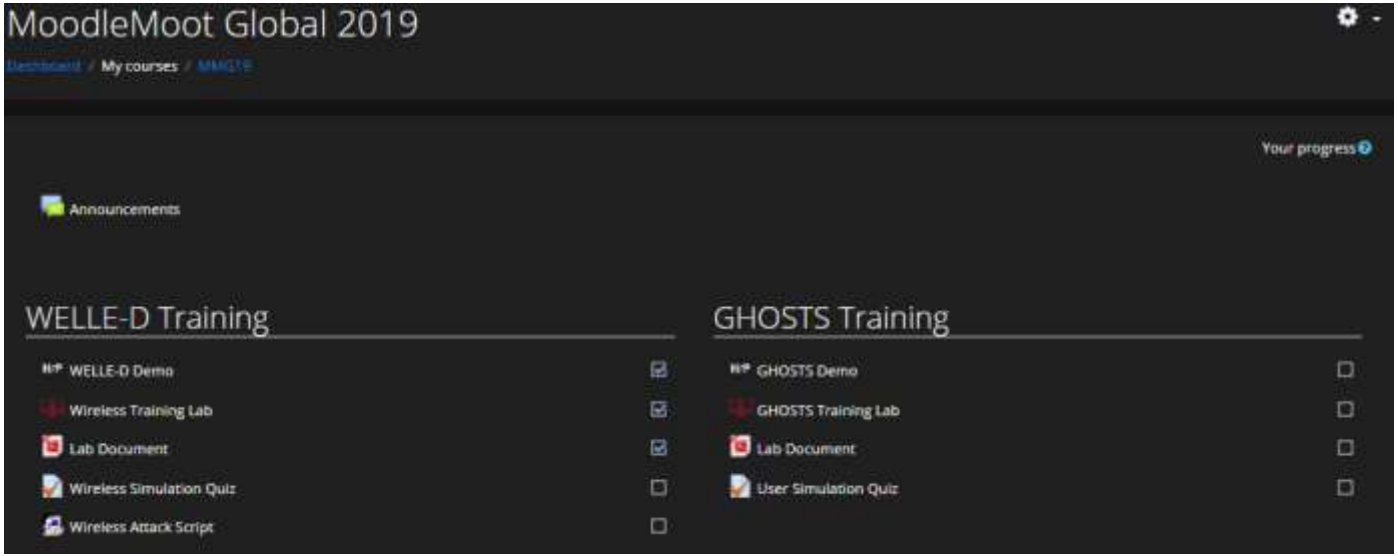
- Content Sync
- Communicates with content discovery system, Foundry
- Automatically informs Foundry of new and updated content
- Type: admin tool
- OAUTH2
- Scheduled tasks

Moodle Development

- Custom Theme
- Matches the rest of our websites that use a dark theme
- Type: theme
- Boost
- Renderers override some content and rearrange course listings
- Looks for values set by local metadata plugin to display embedded activity

Moodle Development

- Custom Theme and course format board

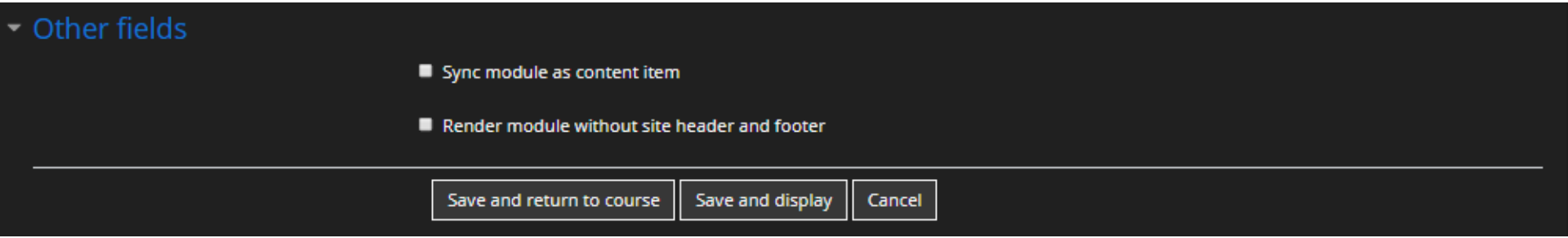


Moodle Development

- Local Metadata
- Used to determine whether to sync content to Foundry
- Used to determine whether to display activity as embedded

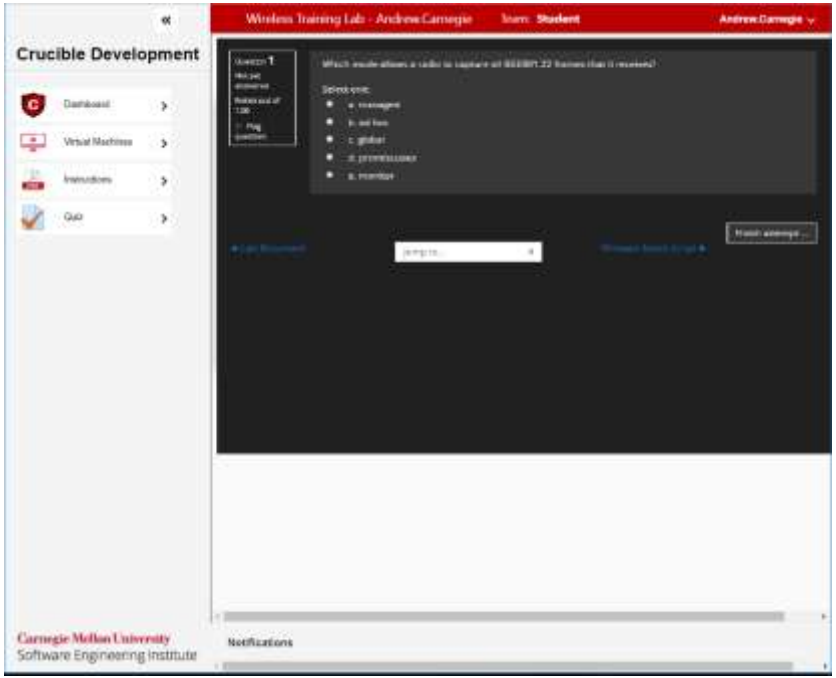
Moodle Development

- Local Metadata



Moodle Development

- Crucible and Local Metadata

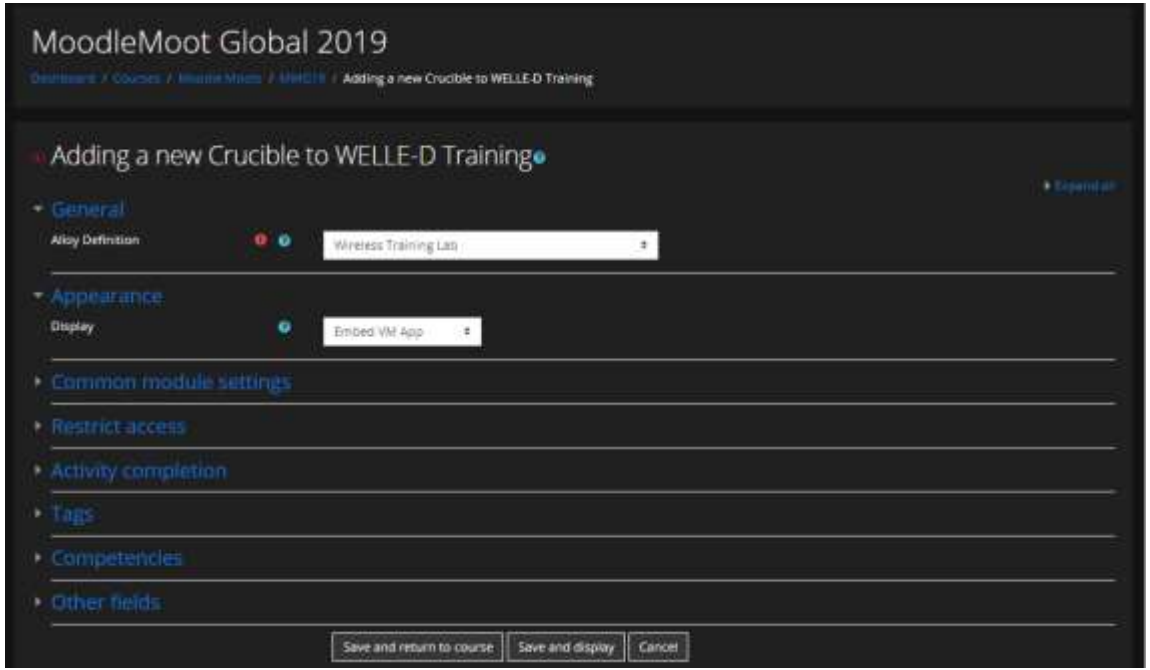


Moodle Development

- Crucible Lab Access
- Communicates with cyber range tool, Crucible
- Allows course creators to select lab from a list of available labs
- Pulls name and deception of lab from Crucible
- Embeds VM consoles or links to a few player view
- Type: activity
- OAUTH2

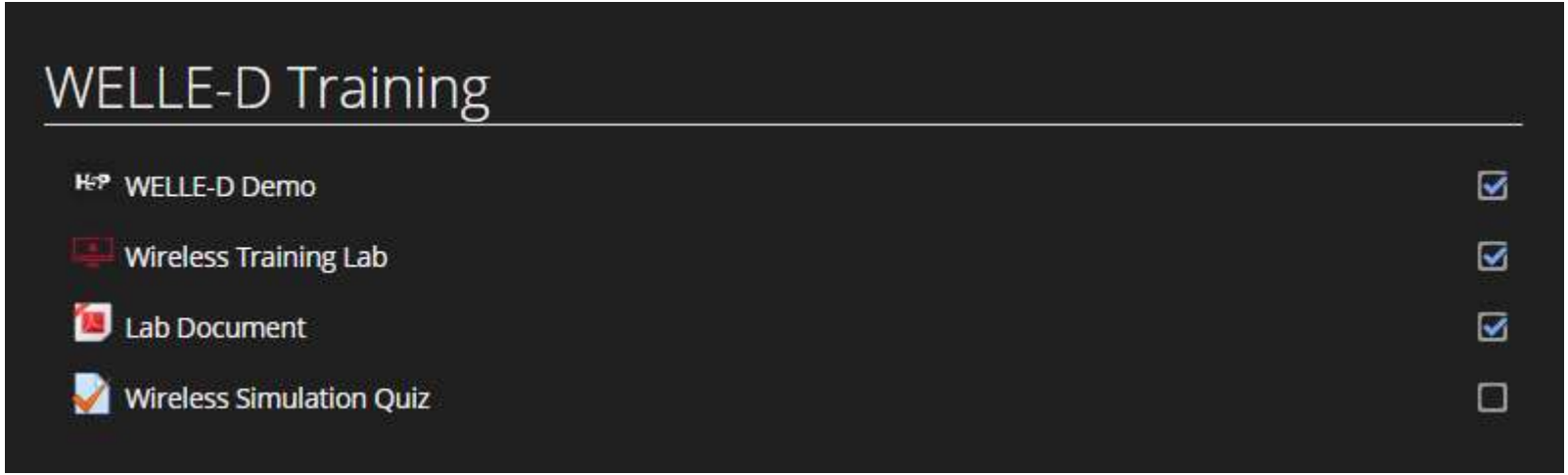
Moodle Development

- Crucible



Moodle Development

- Crucible

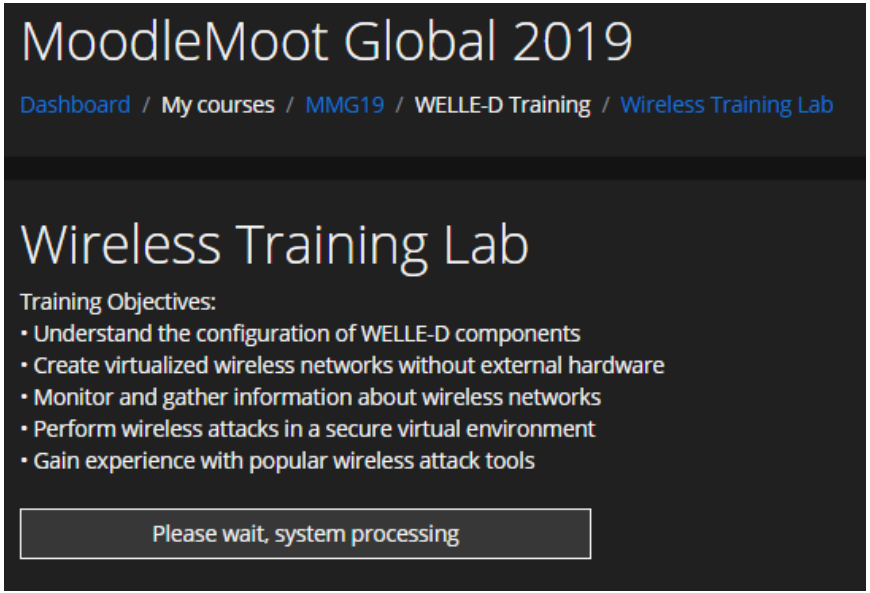


Moodle Development

- Crucible

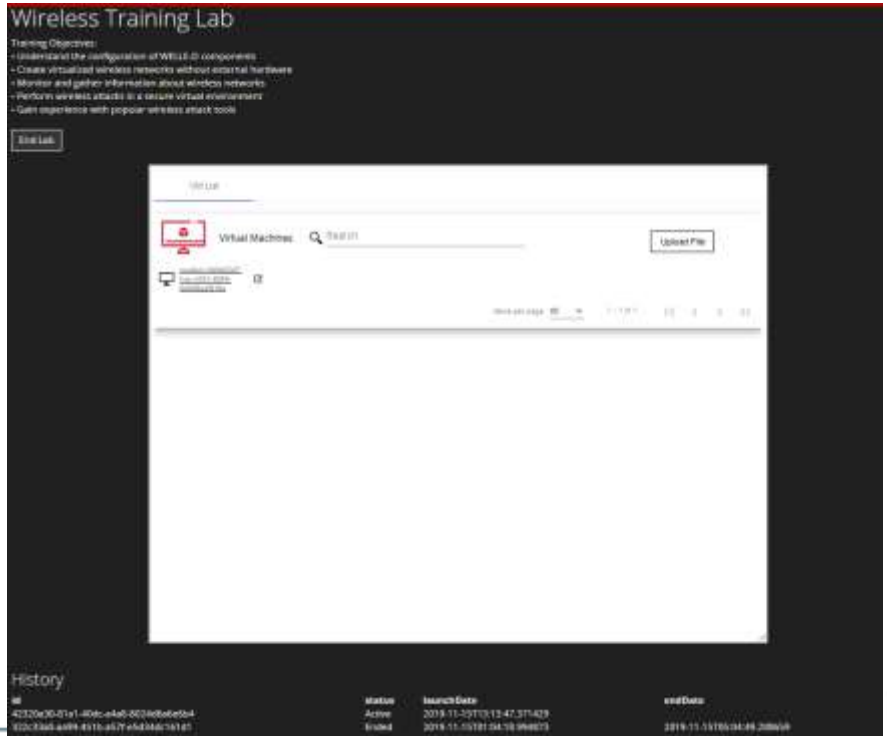
Moodle Development

- Crucible



Moodle Development

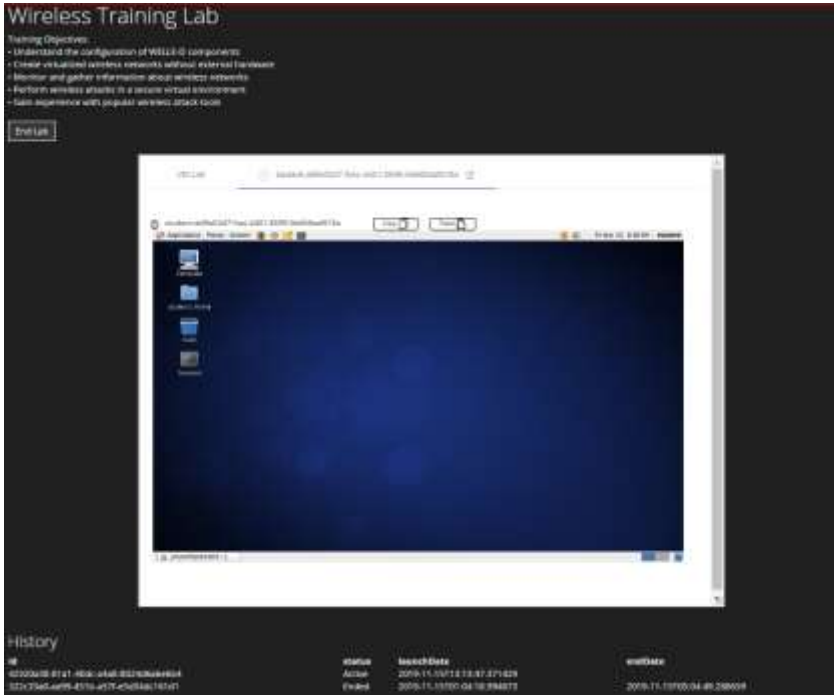
- Crucible



moodlemoot

Moodle Development

- Crucible



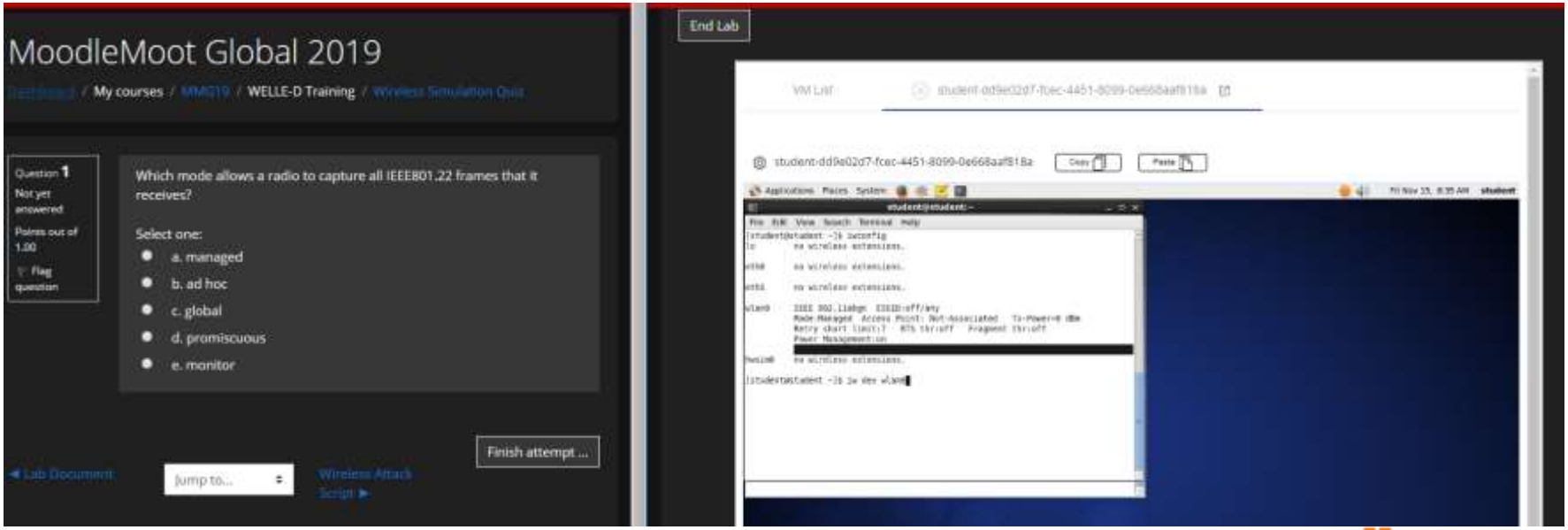
moodlemoot

Moodle Development

- Future integration with Crucible
- Grading of lab tasks
- vTunnel and stackstorm-based Crucible component
- Moodle events and XAPI

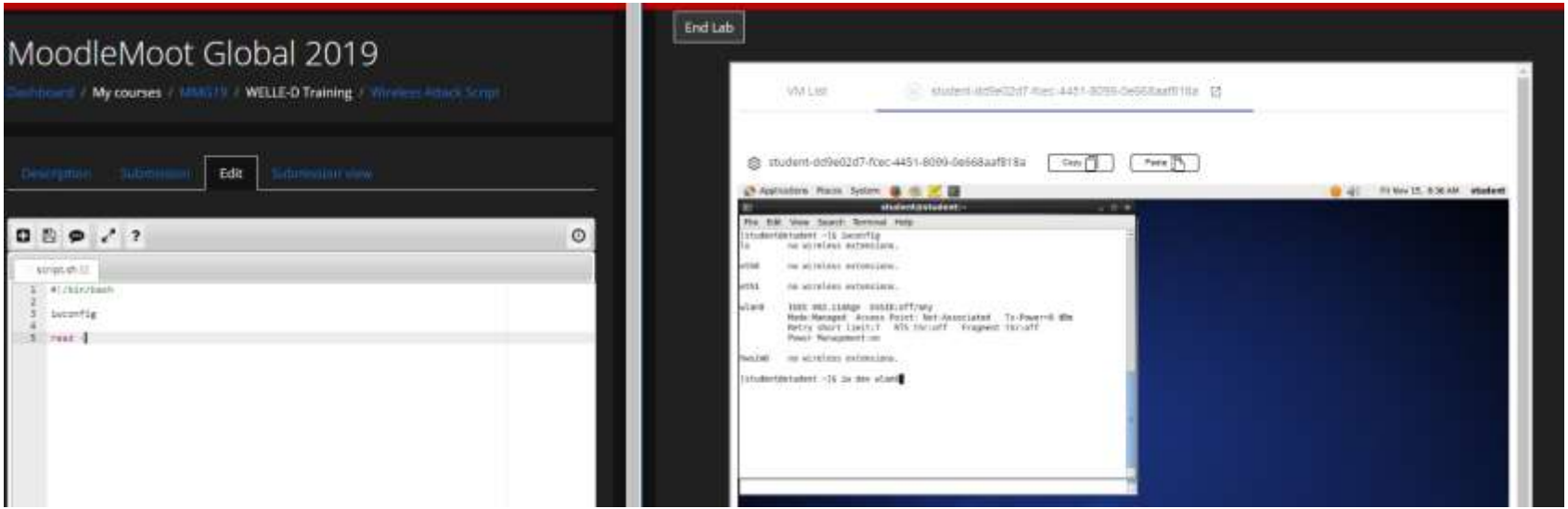
Moodle Development

- Quiz



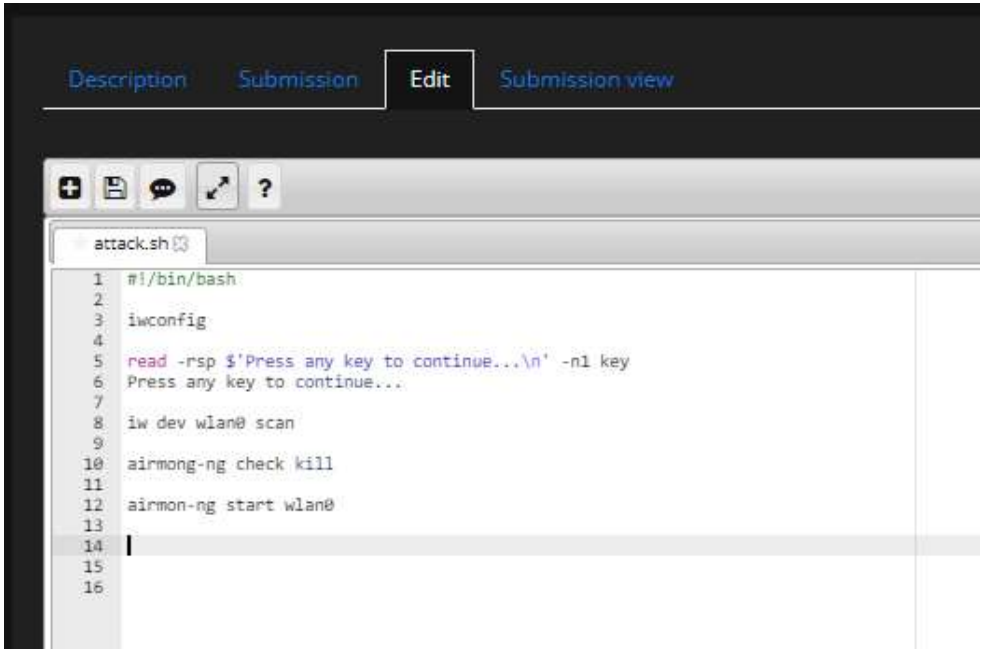
Moodle Development

- VPL



Moodle Development

- VPL



Moodle

- Lab Document

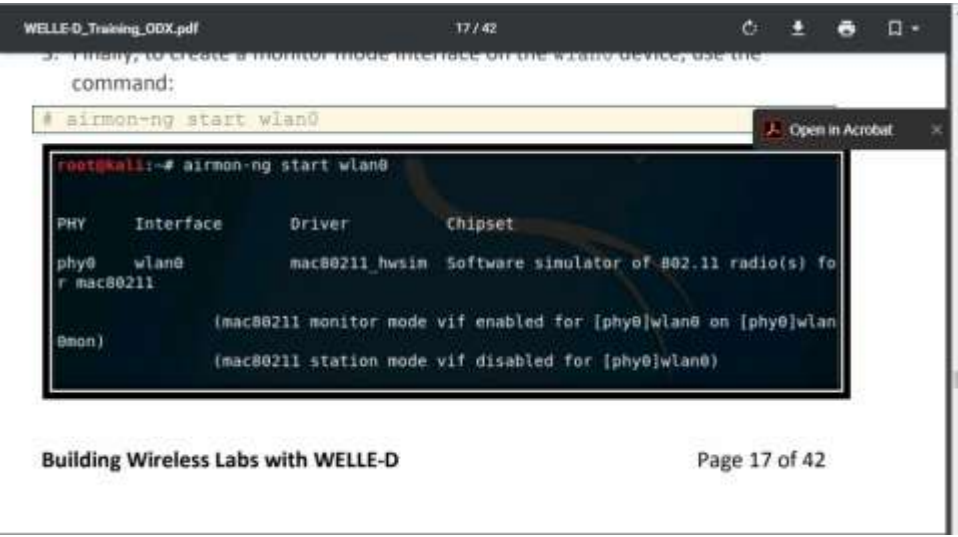
3. Finally, to create a monitor mode interface on the `wlan0` device, use the command:

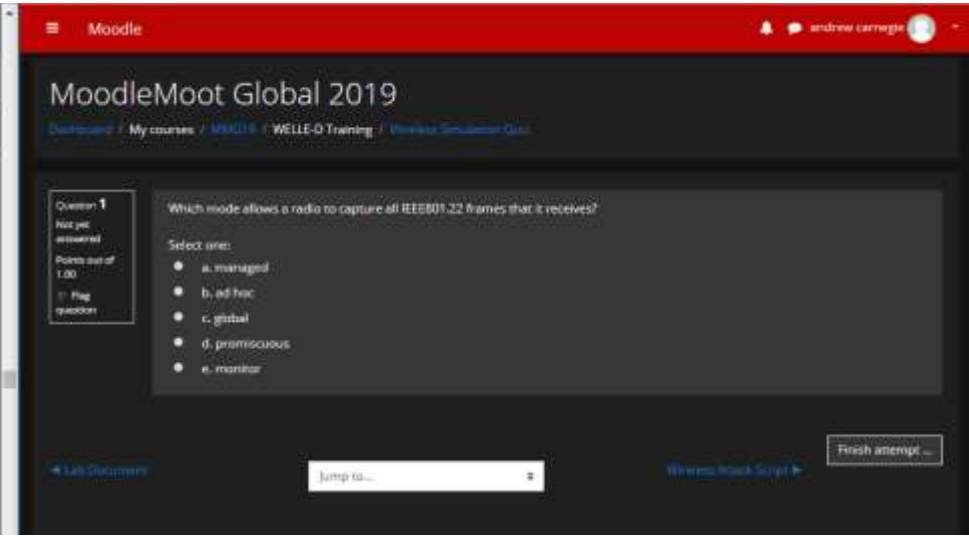
```
# airmon-ng start wlan0
```

```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           mac80211_hwsim  Software simulator of 802.11 radio(s) fo
r mac80211

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

Moodle

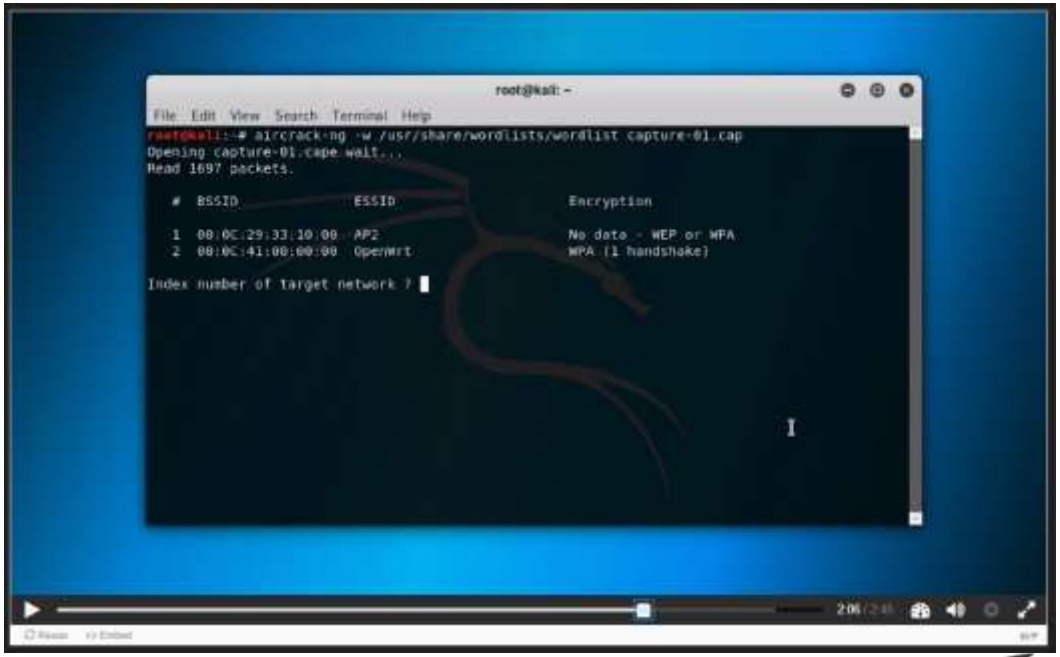
- Lab Document





Moodle

- H5P



http://cmu-sei.github.io