



Virtual Cyber Exercises with Moodle

Adam Welle and Kimo Bumanglag
Carnegie Mellon University

Copyright 2019 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Agenda

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



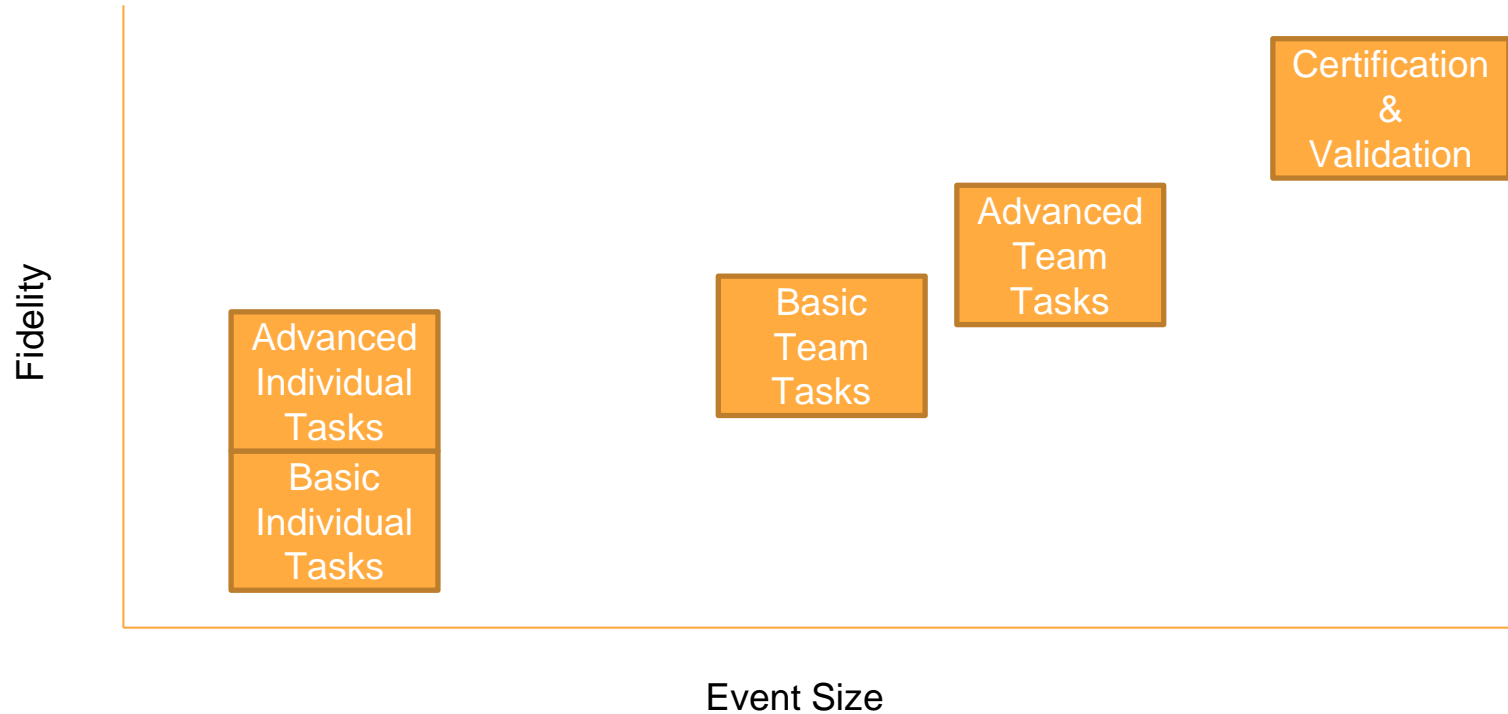
Introduction

- Who we are
- What we do





Cyber Exercise Overview



Range Technologies



Deprecating



TopoMojo

Open Source Lab Builder

Crucible

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

Assessing Performance

Assessment

- LMS – Moodle, of course!
- LRS – Learning Locker
- xAPI – from Moodle, H5P, and VMs
- MELK – Moodle, Elasticsearch, Logstash, Kibana to visualize performance
- NICE Cyber Security Workforce Framework



Assessment with Moodle

Activities

- Quiz
- Feedback
- Files

Features

- Competencies

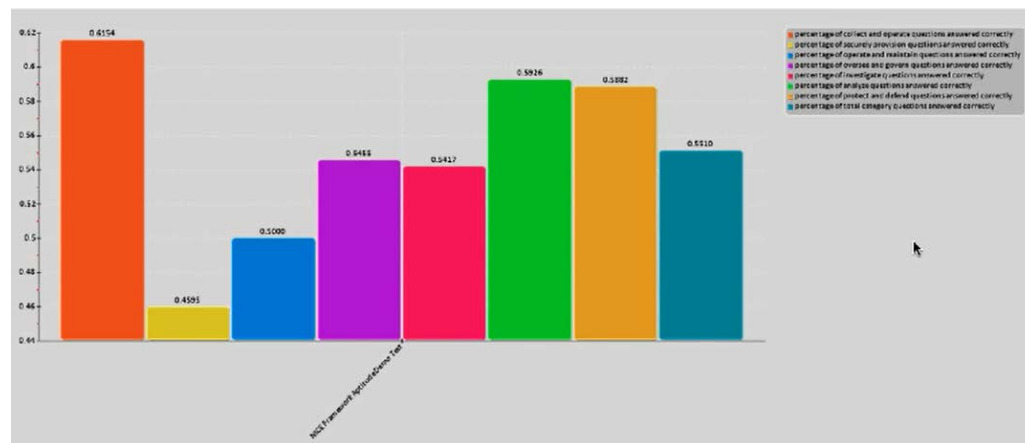
Plugins

- H5P
- Virtual Programming Lab
- Course Format Board
- Logstore xAPI
- Local Metadata



Moodle Competencies

- Cyber Evaluator Tool Output





Custom Integrations with Moodle

- Import courses from old STEP LMS
- Match organizational branding
- Display Moodle content on other systems
- Provide access to VM consoles
- Categorize training and identify skill gaps



Moodle Development

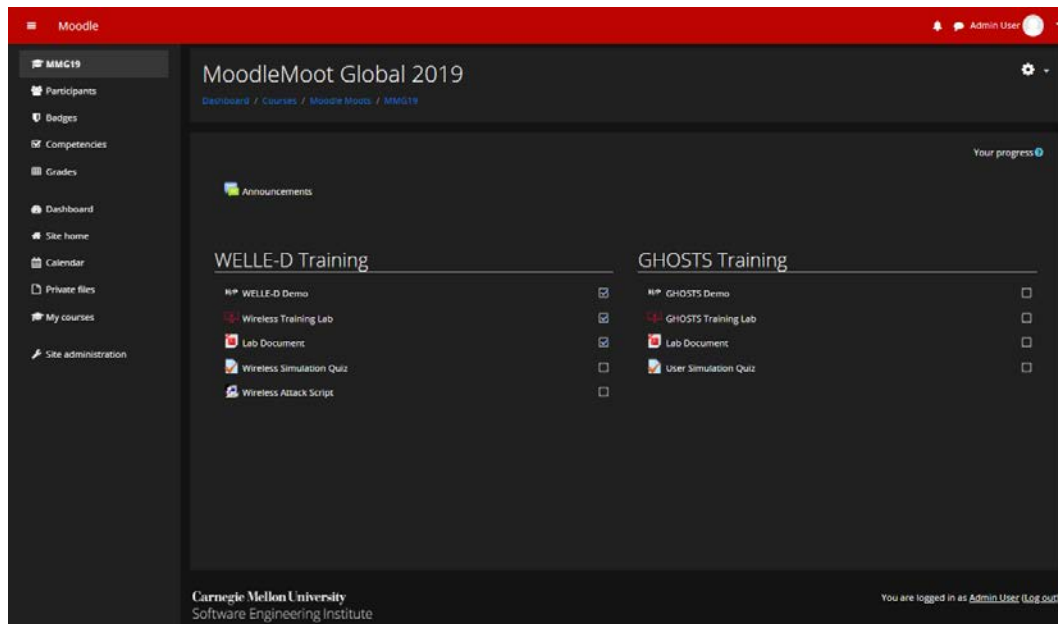
- Content Sync Plugin
- Purpose: Add Moodle content to the Foundry content discovery system
- Type: admin tool
- Leverages: OAUTH2, scheduled tasks
- Communicates with the Foundry API to add content links and images

Moodle Development

- Custom Theme Plugin
- Purpose: Provide a dark theme to match other sites
- Type: theme
- Leverages: Boost theme, local metadata plugin
- Automatically redirects users to OAUTH2 identity server
- Renderer overrides H5P logo with activity logo
- Renderer overrides and rearranges course listing display
- Renderer uses local metadata plugin to override page layout for activities

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

Other fields

- Sync module as content item
- Render module without site header and footer

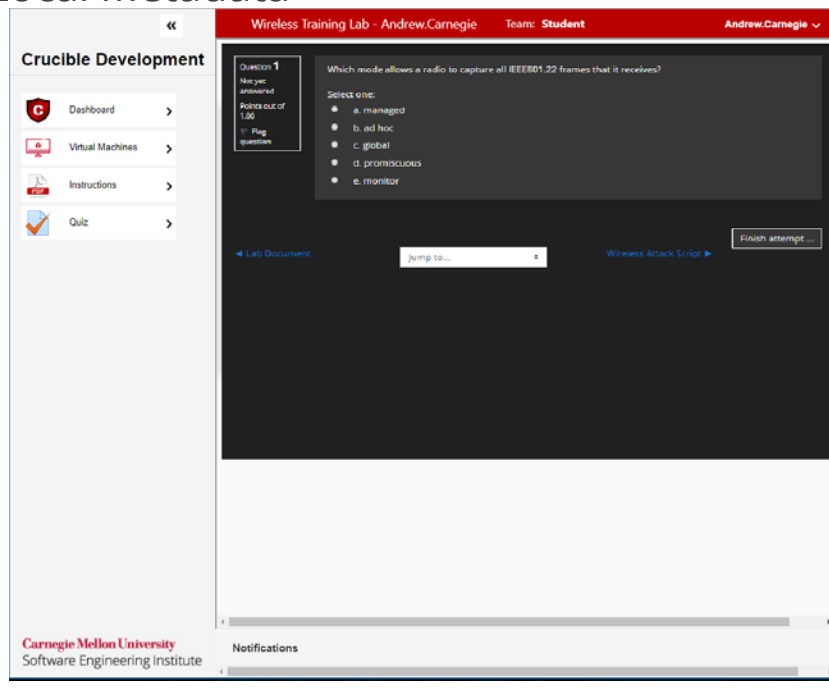
Save and return to course

Save and display

Cancel

Moodle Development

- Crucible and Local Metadata



The screenshot displays the Moodle development interface. On the left is a sidebar for 'Crucible Development' with navigation links: Dashboard, Virtual Machines, Instructions, and Quiz. The main content area shows a quiz question titled 'Question 1' with the text: 'Which mode allows a radio to capture all IEEE801.11 frames that it receives?'. Below the question, there are five radio button options: a. managed, b. ad hoc, c. global, d. promiscuous, and e. monitor. At the bottom of the question area, there is a 'Finish attempt ...' button. The interface also includes a 'Lab Document' link, a 'jump to...' search box, and a 'Wireless Attack Script' link. The top navigation bar shows 'Wireless Training Lab - Andrew.Carnegie', 'Team: Student', and 'Andrew.Carnegie'. The footer contains 'Carnegie Mellon University Software Engineering Institute' and a 'Notifications' section.

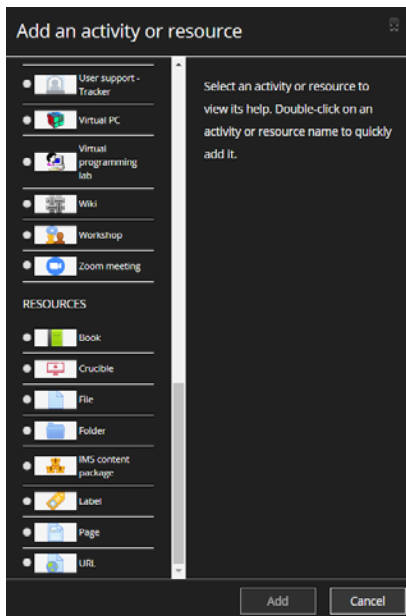


Moodle Development

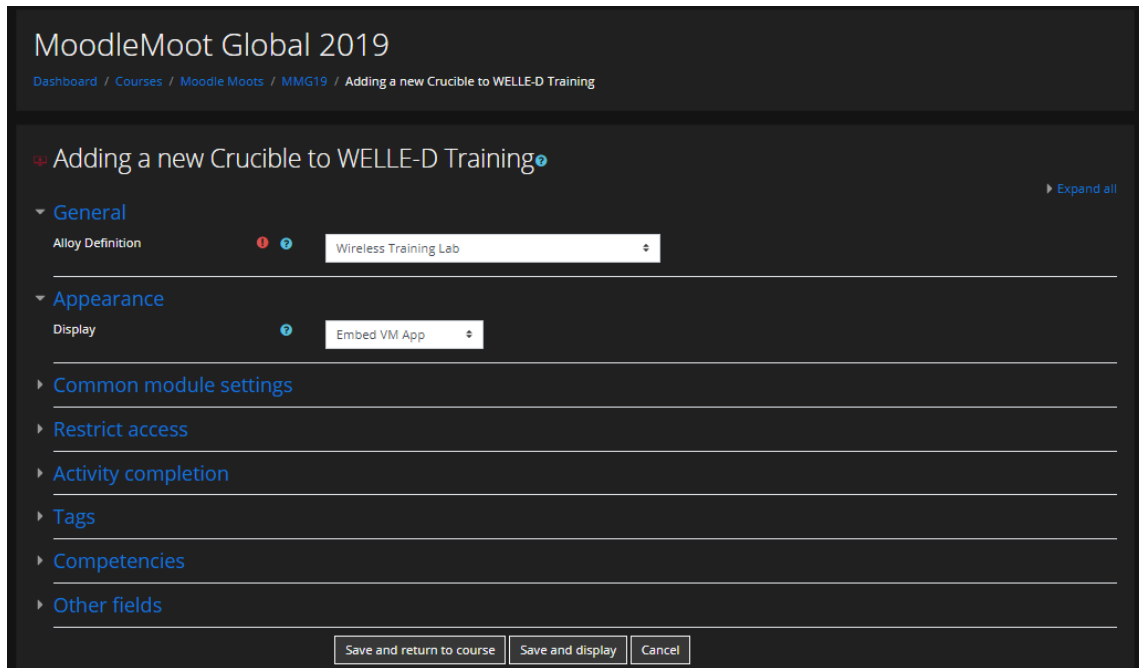
- Crucible Plugin
- Purpose: Deploy labs and access VM consoles
- Type: activity
- Leverages: OAUTH2
- Allows course creators to add lab as a Moodle course activity
- Communicates with the Crucible API
- Pulls name and description of lab from Crucible
- Pulls lab history from Crucible
- Embeds Crucible VM consoles or links to the full Crucible Player

Moodle Development

- Crucible



The screenshot shows the 'Add an activity or resource' dialog box in Moodle. On the left, there is a list of activity and resource icons. Under the 'RESOURCES' section, the 'Crucible' icon is highlighted. On the right, there is a text area with the instruction: 'Select an activity or resource to view its help. Double-click on an activity or resource name to quickly add it.' At the bottom of the dialog, there are 'Add' and 'Cancel' buttons.



The screenshot shows the MoodleMoot Global 2019 course page. The breadcrumb trail is: Dashboard / Courses / Moodle Moots / MMG19 / Adding a new Crucible to WELLE-D Training. The page title is 'Adding a new Crucible to WELLE-D Training'. There is an 'Expand all' link on the right. The configuration is divided into sections: 'General' with 'Alloy Definition' set to 'Wireless Training Lab'; 'Appearance' with 'Display' set to 'Embed VM App'; and several collapsed sections: 'Common module settings', 'Restrict access', 'Activity completion', 'Tags', 'Competencies', and 'Other fields'. At the bottom, there are three buttons: 'Save and return to course', 'Save and display', and 'Cancel'.

Moodle Development

- Crucible



MoodleMoot Global 2019

[Dashboard](#) / [My courses](#) / [MMG19](#) / [WELLE-D Training](#) / [Wireless Training Lab](#)

Wireless Training Lab

Training Objectives:

- Understand the configuration of WELLE-D components
- Create virtualized wireless networks without external hardware
- Monitor and gather information about wireless networks
- Perform wireless attacks in a secure virtual environment
- Gain experience with popular wireless attack tools

[Launch Lab](#)



Moodle Development

- Crucible

MoodleMoot Global 2019

[Dashboard](#) / [My courses](#) / [MMG19](#) / [WELLE-D Training](#) / [Wireless Training Lab](#)

Wireless Training Lab

Training Objectives:

- Understand the configuration of WELLE-D components
- Create virtualized wireless networks without external hardware
- Monitor and gather information about wireless networks
- Perform wireless attacks in a secure virtual environment
- Gain experience with popular wireless attack tools

Please wait, system processing



Moodle Development

- Crucible

Wireless Training Lab

Training Objectives:

- Understand the configuration of WELLE-D components
- Create virtualized wireless networks without external hardware
- Monitor and gather information about wireless networks
- Perform wireless attacks in a secure virtual environment
- Gain experience with popular wireless attack tools

End Lab

VM List

Virtual Machines

Items per page: 50 1-1 of 1

History

id	status	launchDate	endDate
42320a30-81a1-40dc-a4a8-8024df6a6e6d4	Active	2019-11-15T13:13:47.371429	
322c33e0-aa99-451b-a57f-e5d34dc161d1	Ended	2019-11-15T01:04:18.994873	2019-11-15T05:04:49.288659



Moodle Development

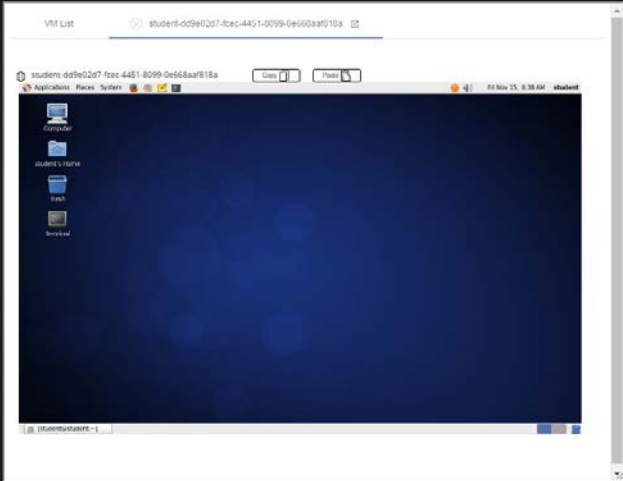
- Crucible

Wireless Training Lab

Training Objectives:

- Understand the configuration of WELLE-D components
- Create virtualized wireless networks without external hardware
- Monitor and gather information about wireless networks
- Perform wireless attacks in a secure virtual environment
- Gain experience with popular wireless attack tools

End Lab

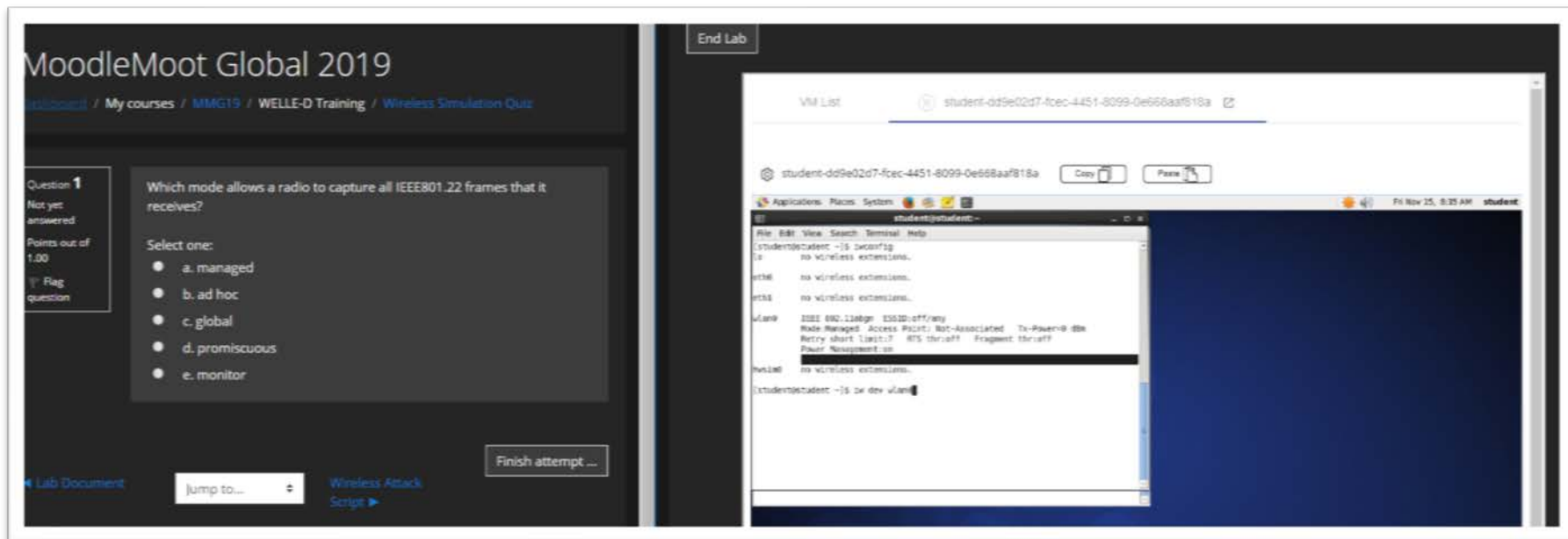


VM List

ID	Status	LaunchDate	EndDate
42320a30-81a1-40dc-a4a8-8024d6e6e694	Active	2019-11-14 15:13:13.47.371429	
322c33a0-a499-451b-a57f-e5d34dc161d1	Ended	2019-11-15 10:04:18.994873	2019-11-15 10:05:04:49.288659

Moodle Layout

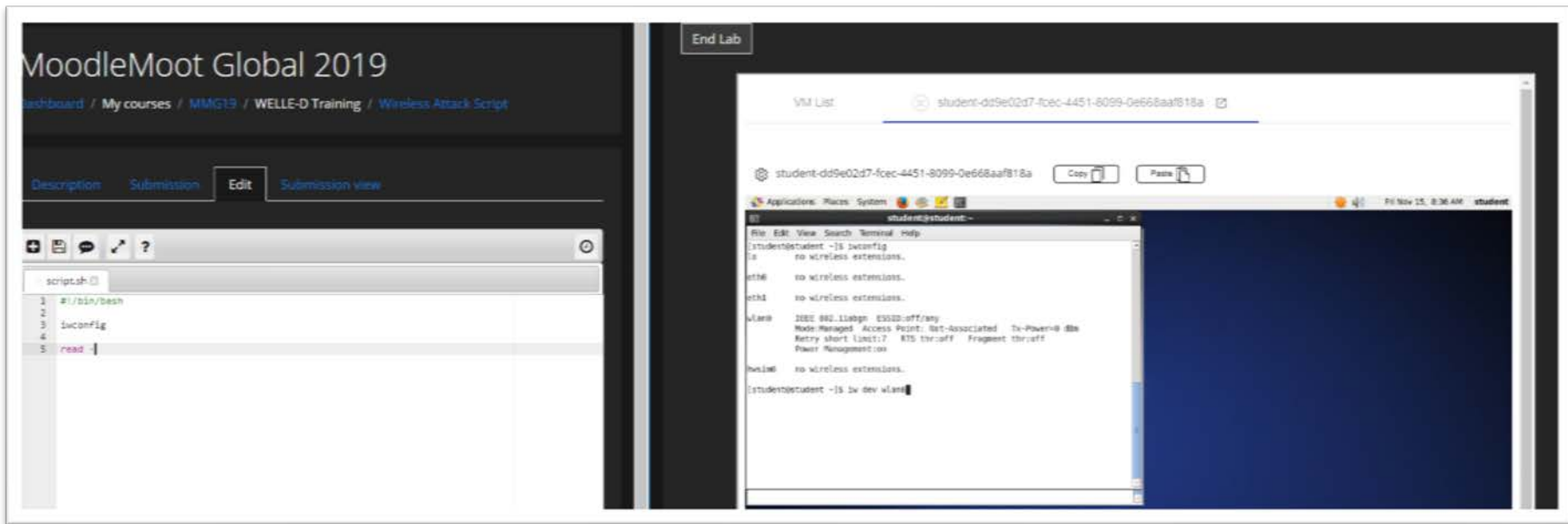
- Quiz



The image shows two side-by-side screenshots from a MoodleMoot Global 2019 lab. The left screenshot displays a quiz question: "Which mode allows a radio to capture all IEEE801.22 frames that it receives?" with five radio button options: a. managed, b. ad hoc, c. global, d. promiscuous, and e. monitor. The right screenshot shows a terminal window with the command `iwconfig` and its output, which lists network interfaces (eth0, eth1, wlan0, wlan1) and their configurations, including the `mode Managed` for wlan0.

Moodle Layout

- VPL



The screenshot displays the Moodle VPL (Virtual Practice Lab) interface. On the left, the Moodle course page is visible, titled "MoodleMoot Global 2019". The breadcrumb trail shows the path: "Dashboard / My courses / MMG19 / WELLE-D Training / Wireless Attack Script". Below the breadcrumb, there are tabs for "Description", "Submission", "Edit", and "Submission view". The "Edit" tab is active, showing a code editor with a file named "script.sh". The code in the editor is as follows:

```
1 #!/bin/bash
2
3 iwconfig
4
5 read
```

On the right, a terminal window is open, showing the execution of the script. The terminal output is:

```
VM List: student-dd9e02d7-fcec-4451-8099-0e668aaf818a
Copy Paste
student-dd9e02d7-fcec-4451-8099-0e668aaf818a
Applications Places System
student@student-
File Edit View Search Terminal Help
[student@student ~]$ iwconfig
ls
eth0 no wireless extensions.
eth1 no wireless extensions.
eth2 no wireless extensions.
wlan0 IEEE 802.11abgn ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=0 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on
[student@student ~]$ iw dev wlan0
```


Future Moodle Development

- Further integration with Crucible
- Moodle events and xAPI
- Grading of lab tasks automatically
- Release Crucible and mod_crucible on Github in 2020



<http://cmu-sei.github.io>