



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.
DM19-1210

Legal slide

Agenda

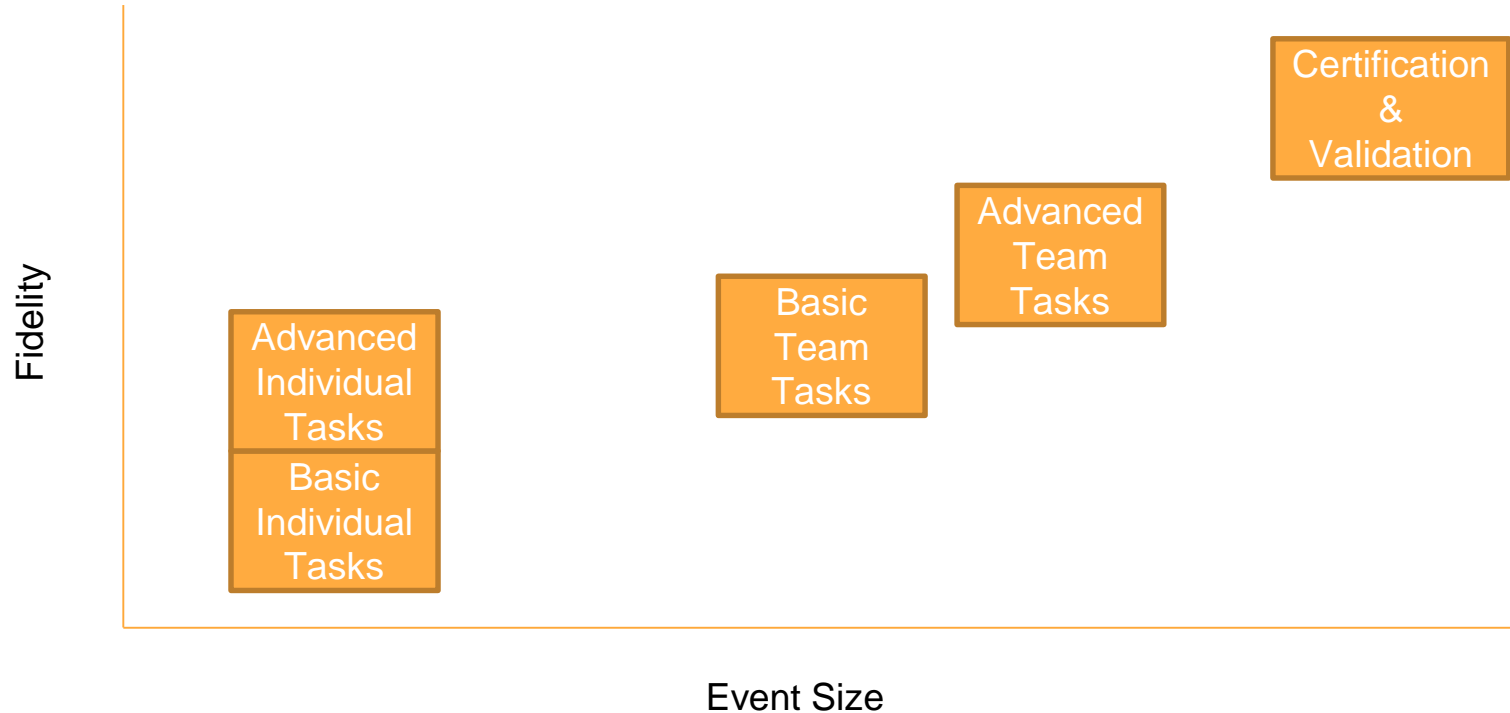
- Introduction
- Cyber Exercise Overview
- Training Objectives
- Range Technologies
- Simulations
- Integrating with Moodle

Introduction

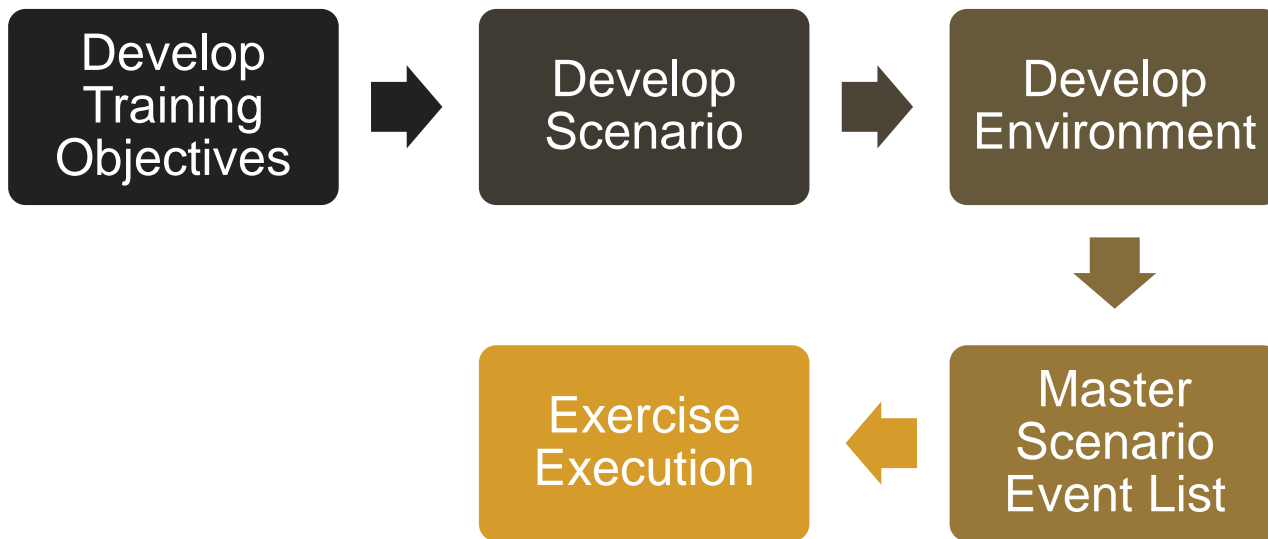
- Who we are
- What we do



Cyber Exercise Overview



Training Objectives



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

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

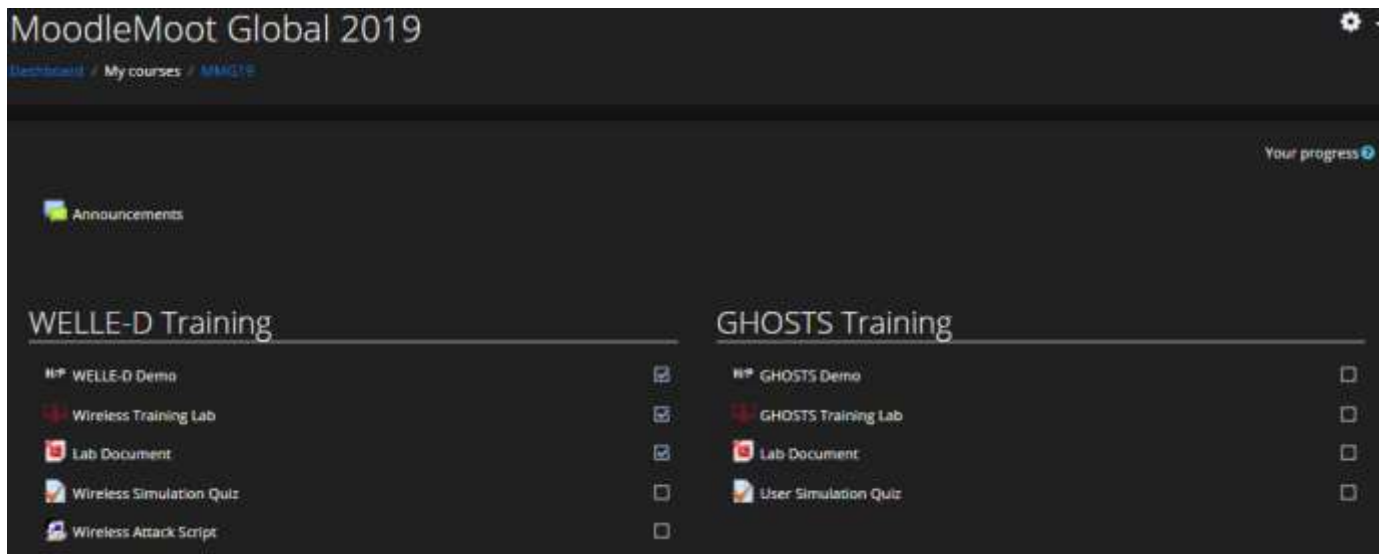
- Content Sync
- Communicates with content discovery system, Foundry
- Automatically informs Foundry of new and updated content
- Type: admin tool
- OAUTH2
- Scheduled tasks

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



The screenshot displays the MoodleMoot Global 2019 course format board. The interface is dark-themed and includes a navigation bar at the top with the text "MoodleMoot Global 2019" and a settings gear icon. Below the navigation bar, there are breadcrumb links: "Dashboard / My courses / MMGT9". A "Your progress" indicator is visible in the top right corner. The main content area is divided into two columns: "WELLE-D Training" and "GHOSTS Training". Each column contains a list of course items with icons and checkboxes. The "WELLE-D Training" column lists: "WELLE-D Demo" (with a checkmark), "Wireless Training Lab" (with a checkmark), "Lab Document" (with a checkmark), "Wireless Simulation Quiz" (with an unchecked checkbox), and "Wireless Attack Script" (with an unchecked checkbox). The "GHOSTS Training" column lists: "GHOSTS Demo" (with an unchecked checkbox), "GHOSTS Training Lab" (with an unchecked checkbox), "Lab Document" (with an unchecked checkbox), and "User Simulation Quiz" (with an unchecked checkbox).

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

Other fields

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

Save and return to course

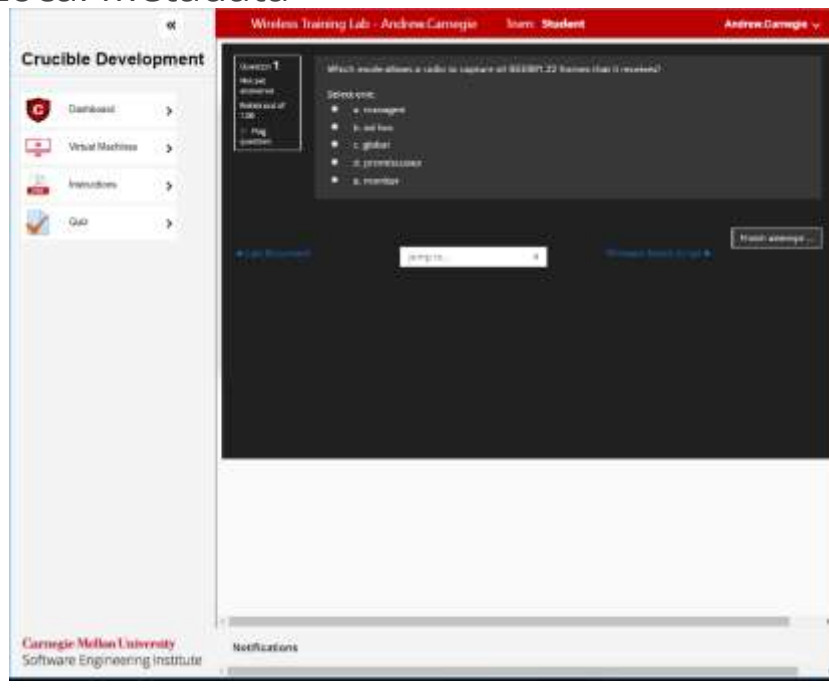
Save and display

Cancel



Moodle Development

- Crucible and Local Metadata

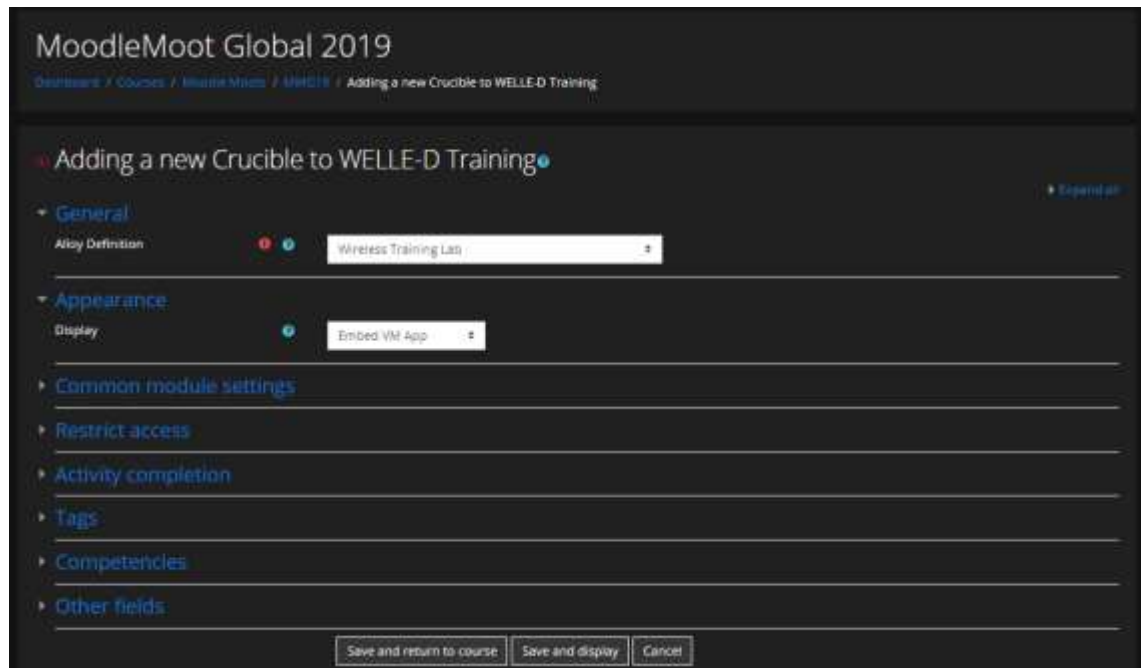
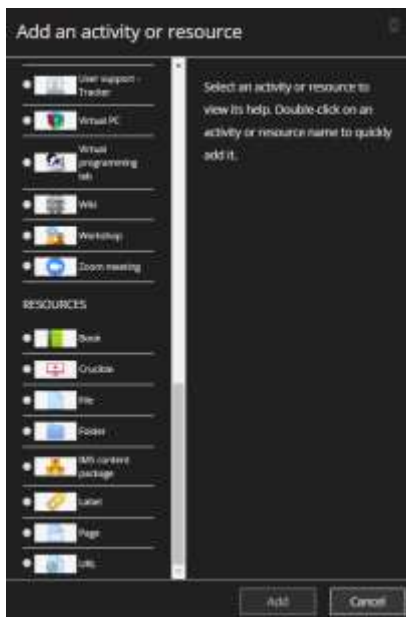


Moodle Development

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

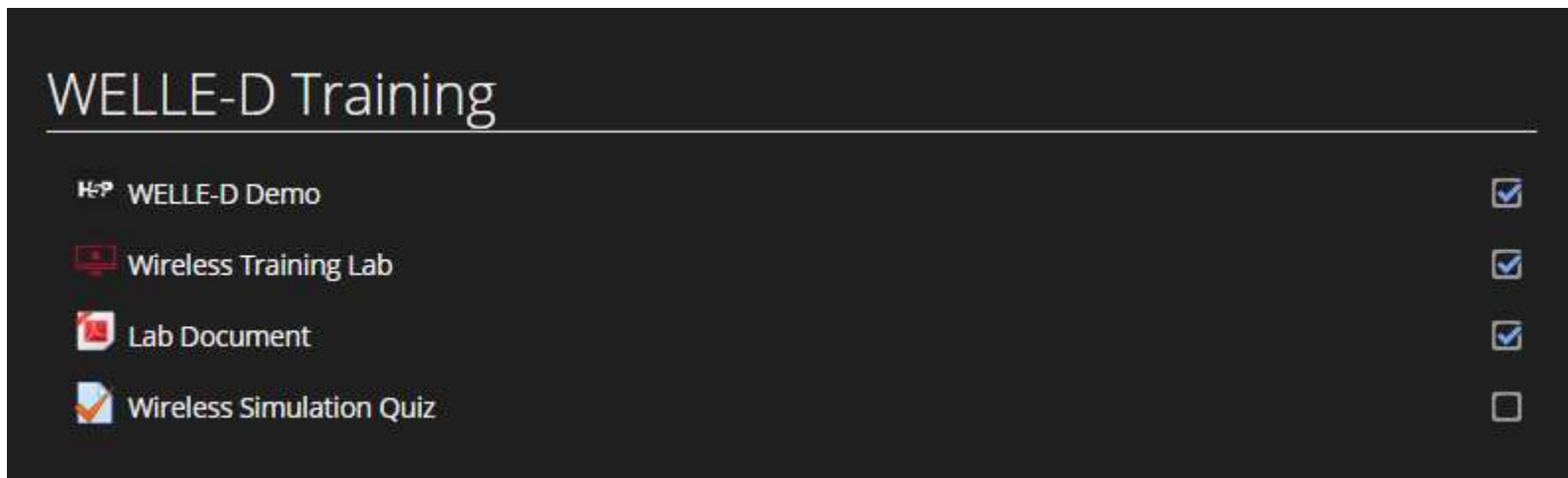
Moodle Development

- Crucible



Moodle Development

- Crucible



The screenshot shows a Moodle course page titled "WELLE-D Training". Below the title, there is a list of four course activities, each with a small icon and a checkbox on the right. The activities are:

- WELLE-D Demo (with a document icon) - checked
- Wireless Training Lab (with a computer monitor icon) - checked
- Lab Document (with a document icon) - checked
- Wireless Simulation Quiz (with a checkmark icon) - unchecked

Moodle Development

- Crucible

A screenshot of a Moodle course page for MoodleMoot Global 2019. The page has a dark grey background with white text. At the top, it says "MoodleMoot Global 2019" in a large font. Below that is a breadcrumb trail: "Dashboard / My courses / MMG19 / WELLE-D Training / Wireless Training Lab". The main heading is "Wireless Training Lab". Underneath, it lists "Training Objectives:" followed by five bullet points. At the bottom left, there is a "Launch Lab" button.

MoodleMoot Global 2019

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

Wireless Training Lab

Training Objectives:

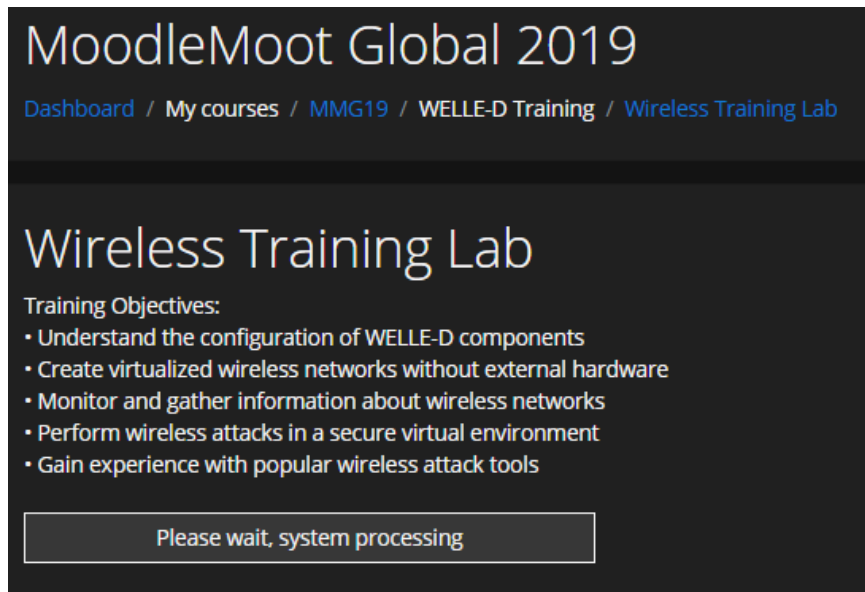
- Understand the configuration of WELLE-D components
- Create virtualized wireless networks without external hardware
- Monitor and gather information about wireless networks
- Perform wireless attacks in a secure virtual environment
- Gain experience with popular wireless attack tools

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

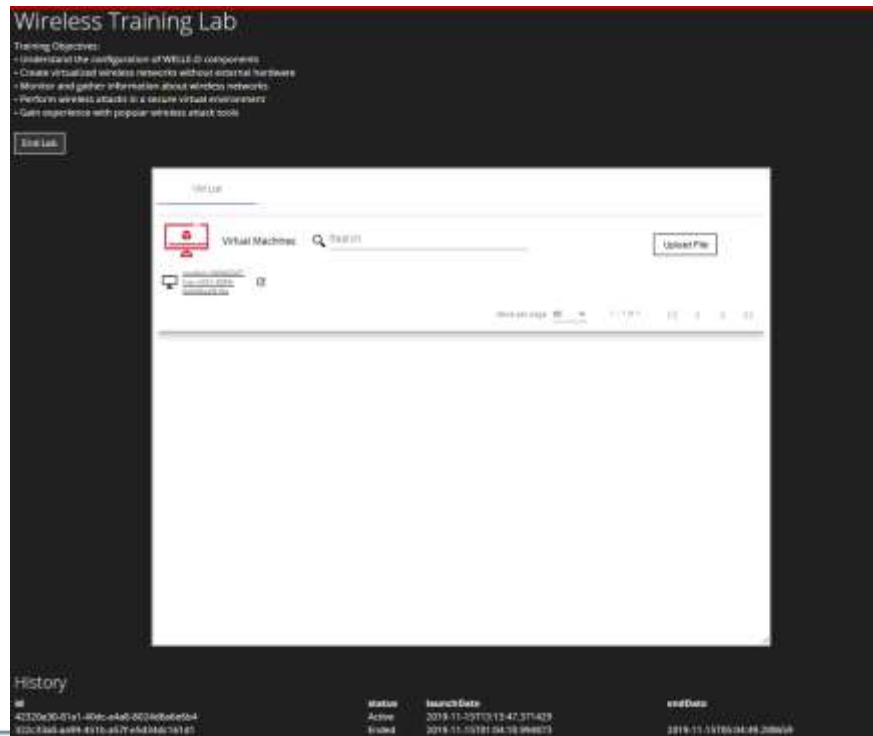
- Crucible

Wireless Training Lab

Training Objectives:

- Understand the configuration of Wi-Fi 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

Start Lab



ID	Status	Search Date	end Date
42320e90-01e1-40dc-e460-0030466e0e04	Active	2019-11-20T10:13:47.371429	
62c33ad-a094-451b-a577-e6d3d6c78185	Enrolled	2019-11-15T01:04:18.966873	2019-11-15T05:04:48.208668

Moodle Development

- Crucible

Wireless Training Lab

Training Objectives:

- Understand the configuration of Wireless-2000 computers
- Create virtualized wireless networks within a virtual machine
- Monitor and gather information about wireless networks
- Perform wireless attacks in a secure virtual environment
- Gain experience with popular wireless attack tools

[View Lab](#)



History

ID	status	launchDate	endTime
4230240-81a1-4048-8026364e804	Active	2019-11-19T12:13:37.271429	
1207364e804-417b-417c-4048-147d1	Ended	2019-11-19T00:04:16.894072	2019-11-19T00:04:49.148009

Moodle Development

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

Moodle Development

- Quiz

MoodleMoot Global 2019

Dashboard / My courses / MMQ19 / WELLE-D Training / Wireless Simulation Quiz

Question 1
Not yet answered
Points out of 1.00
Flag question

Which mode allows a radio to capture all IEEE802.22 frames that it receives?

Select one:

- a. managed
- b. ad hoc
- c. global
- d. promiscuous
- e. monitor

Lab Document Jump to... Wireless Attack Script

Finish attempt ...

End Lab

VM LINT student-dd9e02d7-fcac-4451-8099-0e668aaf818a

Copy Paste

student-dd9e02d7-fcac-4451-8099-0e668aaf818a

```
File Edit View Search Window Help
[student@student ~]$ sudoconfig
to:
no wireless extensions.

wlan0 no wireless extensions.
wlan1 no wireless extensions.

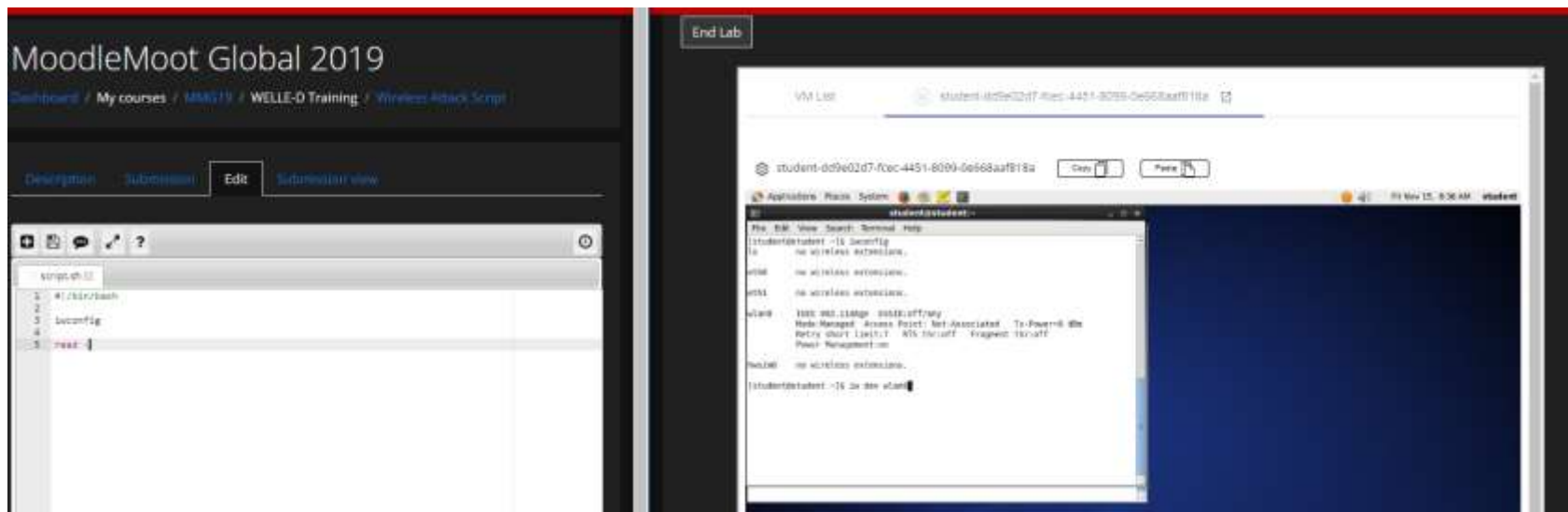
wlan0 IEEE 802.11abgn: ESSID:off/any
Mode Managed Access Point: Not-Associated Tx-Power: 0dB
Retry short limit: 80% Shortoff Fragment Shortoff
Power Management on

wlan1 no wireless extensions.

[student@student ~]$ sudo ifconfig wlan0
```

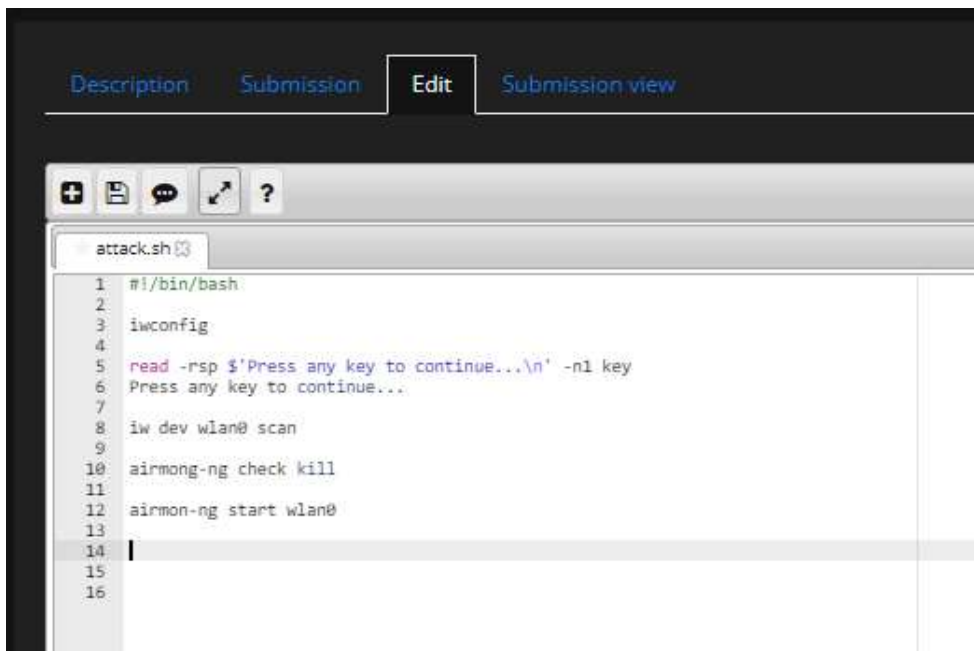
Moodle Development

- VPL



Moodle Development

- VPL



The screenshot shows a Moodle VPL editor interface. At the top, there are four tabs: 'Description', 'Submission', 'Edit' (which is active), and 'Submission view'. Below the tabs is a toolbar with icons for adding, saving, commenting, sharing, and help. The main area displays a shell script named 'attack.sh' with the following content:

```
1 #!/bin/bash
2
3 iwconfig
4
5 read -rsp 'Press any key to continue...\n' -n1 key
6 Press any key to continue...
7
8 iw dev wlan0 scan
9
10 airmong-ng check kill
11
12 airmon-ng start wlan0
13
14 |
15
16
```

Moodle

- Lab Document

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

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

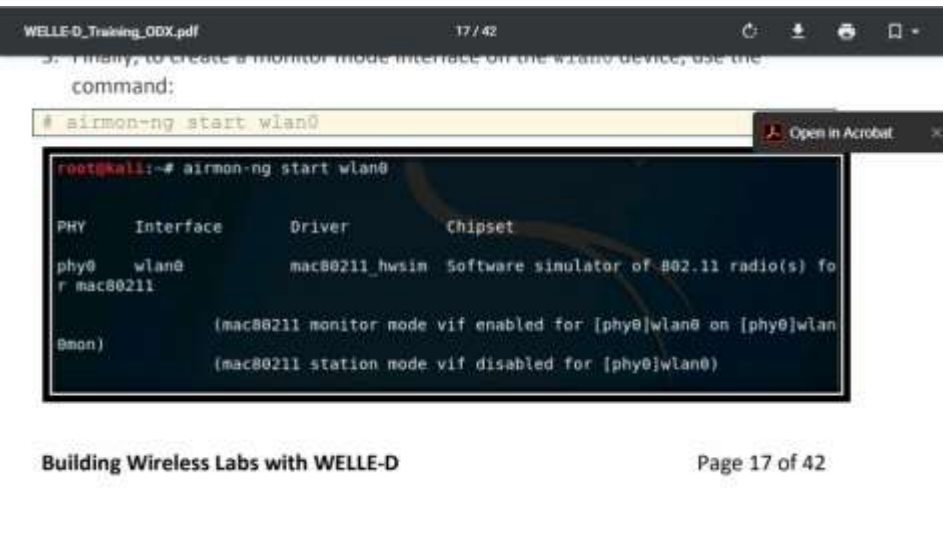
```
root@kali:~# airmon-ng start wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0          mac80211_hwsim  Software simulator of 802.11 radio(s) for
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



WELLE-D_Training_ODX.pdf 17 / 42

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

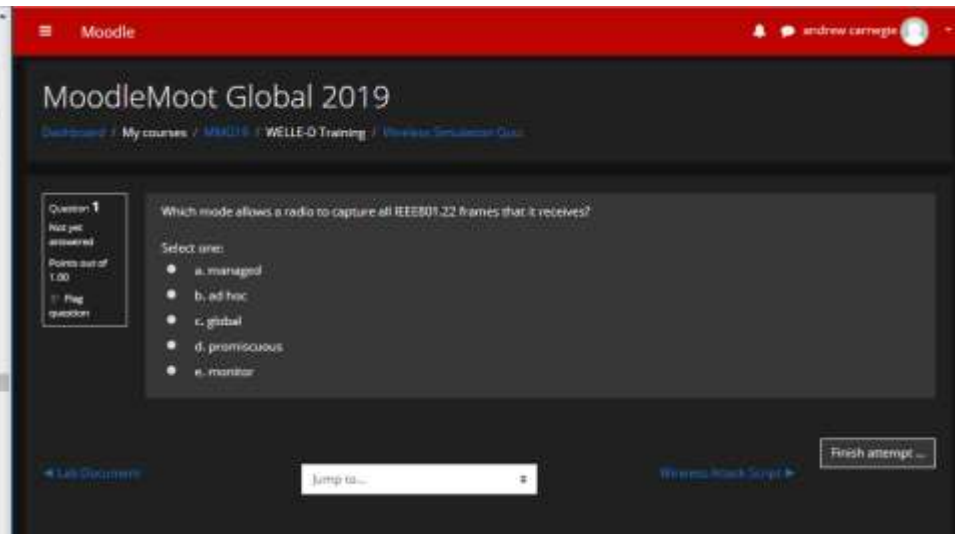
```
# airmon-ng start wlan0
```

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

PHY	Interface	Driver	Chipset
phy0	wlan0	mac80211_hwsim	Software simulator of 802.11 radio(s) for mac80211

```
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
```

Building Wireless Labs with WELLE-D Page 17 of 42



Moodle

MoodleMoot Global 2019

Dashboard / My courses / WELLE-D / WELLE-D Training / Wireless Simulation Course

Question 1
Not yet attempted
Points out of 1.00
Flag question

Which mode allows a radio to capture all IEEE802.11 frames that it receives?

Select one:

- a. managed
- b. ad hoc
- c. global
- d. promiscuous
- e. monitor

4 Lab Documents

Jump to...

Finish attempt ...

Moodle

- H5P

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aircrack-ng -w /usr/share/wordlists/wordlist capture-01.cap  
Opening capture-01.cap: wait...  
Read 1697 packets.  


| # | BSSID             | ESSID   | Encryption           |
|---|-------------------|---------|----------------------|
| 1 | 00:0C:29:33:10:08 | AP2     | No data - WEP or WPA |
| 2 | 00:0C:41:00:00:00 | OperMrt | WPA (1 handshake)    |

  
Index number of target network ?
```



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