Virtual Cyber Exercises with Moodle

Adam Welle and Kimo Bumanglag
Carnegie Mellon University
Agenda

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

- Who we are
- What we do
Cyber Exercise Overview

Event Size

Fidelity

- Basic Individual Tasks
- Advanced Individual Tasks
- Basic Team Tasks
- Advanced Team Tasks
- Certification & Validation

[Distribution Statement A] Approved for public release and unlimited distribution.
Range Technologies

- Deprecating
  - STEP® Fwd
    - CERT Simulation, Training, & Exercise Platform

- Open Source Lab Builder
  - TopoMojo

- Full Scale Environment Builder
  - Crucible
  - Coming soon

[Distribution Statement A] Approved for public release and unlimited distribution.
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

[Distribution Statement A] Approved for public release and unlimited distribution.
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

[Distribution Statement A] Approved for public release and unlimited distribution.
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

- Crucible and Local Metadata
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
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
Moodle Development

- Crucible
Moodle Layout

- Quiz
Moodle Layout

- VPL
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