Carnegie
Mellon
University
Information
Networking
Institute

Continuous Cybersecurity Instruction

Empowering Students to Build Hands-on Labs

Chris Herr, Matt Kaar

2025 NICE Conference, Denver, Colorado

Who Am I?

Chris Herr

- Cybersecurity Exercise Developer, group Lead
  (SEI, CERT, Cyber Mission Readiness)
- Adjunct Instructor
  (Information Networking Institute, Heinz College)
- Research Areas
  - Education & Training
  - Skills-based Assessments
  - Gamification and Video Games as Training Tools
- Prior Work Experience
  - U.S. Army (2004-2008)

Who Am I?

Matt Kaar

- Senior Engineer and Team Lead
  (Software Engineering Institute)
- Adjunct Instructor
  (Information Networking Institute)
- Research Areas
  - Cloud Security
  - Automation
- Prior Work Experience
  - MITRE
  - Federal Aviation Administration
  - Internet Security Systems

Where We Work

About the INI

The INI was founded in 1989 in response to an industry need to forge collaboration between computer scientists and communications engineers.

INI Degree Programs

Pittsburgh

M.S. in Information Networking

M.S. in Information Security*

M.S. in Artificial Intelligence Engineering - Information Security**

Pittsburgh + CMU-SV

M.S. in Mobile and IoT Engineering

M.S. in Information Technology - Information Security

* Recently named #1 in the country by *Fortune*

** Newest program, launched 2022

Excellence in Cybersecurity

M.S. in Information Security is nationally celebrated

Foundation for CMU’s status as a National Center for Academic Excellence in Cybersecurity

Basis for CMU’s federal Scholarship for Service (SFS) program

Named #1 cybersecurity master’s in the U.S. by *Fortune* this year

First degree of its kind in the U.S.

Certificates and Specializations

Cyber Operations

Cyber Operations prepares graduates for crucial cybersecurity service in the government and military.

Cyber Defense

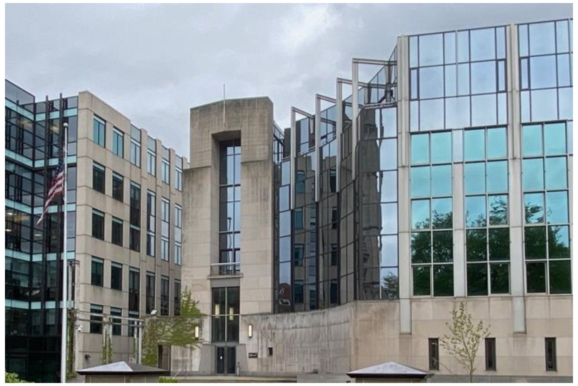
Cyber Defense provides a focused set of skills highly relevant to careers in cybersecurity.

Cyber Forensics and Incident Response (CyFIR)

Taught by instructors from the CMU Software Engineering Institute’s CERT Division, CyFIR prepares students in information security and digital investigations.

Software Engineering Institute

U.S. Department of Defense Research Center



Chartered to perform applied research in:

- **Software engineering**, **Cybersecurity**, and **Artificial Intelligence** (AI)
- Headquartered in Pittsburgh, Pennsylvania on CMU's campus (+ offices near Washington D.C.)
- 650 staff members

The CERT Division at CMU/SEI is the world's first Computer Emergency Response Team, founded in 1988.

Today’s Talk

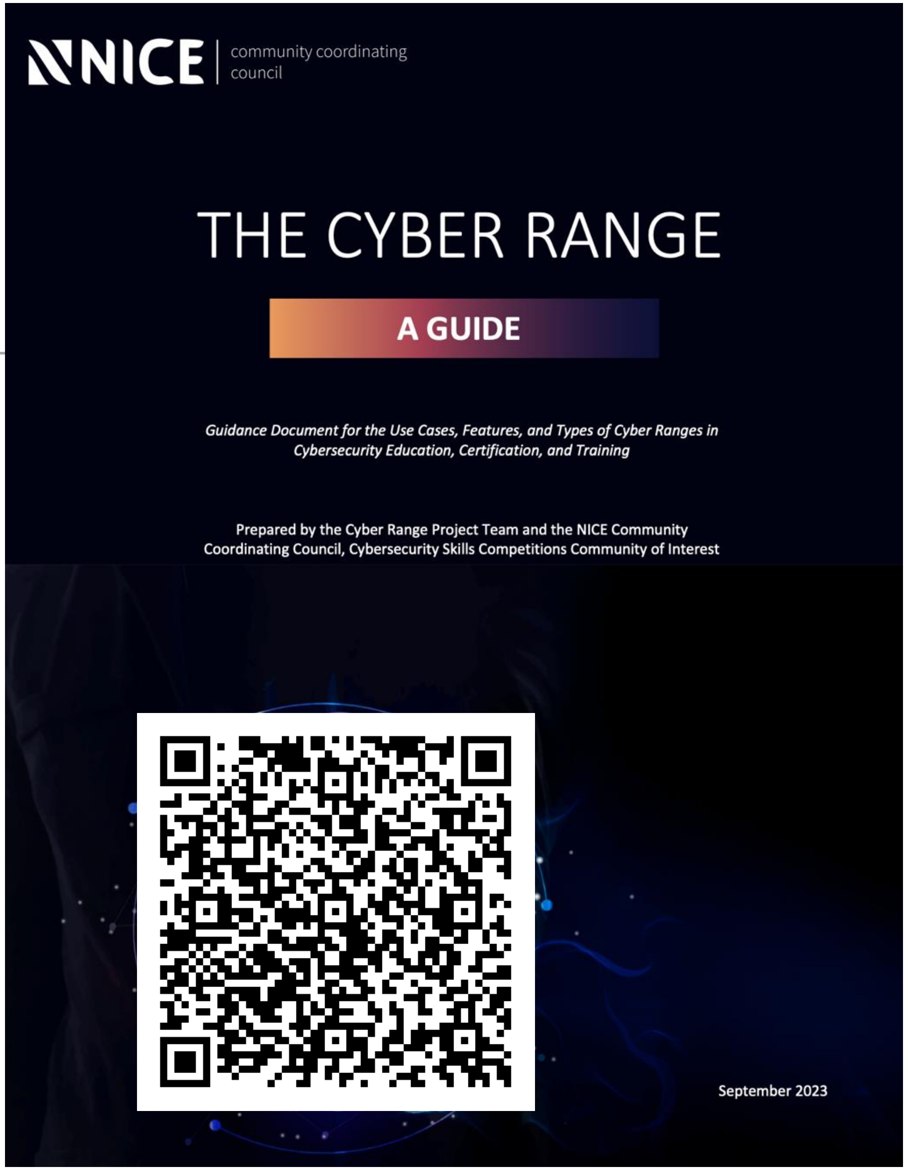
Importance of “Hands-on” Instruction

Tell me and I forget,
teach me and I remember,
involve me and I learn.

–Xun Kuang,
Chinese Confucian philosopher

Hands-on Challenges

- Maintaining hands-on training environments involves significant overhead.
- As technology and cybersecurity techniques evolve, so must the training environments used to teach them.



NICE | community coordinating council

THE CYBER RANGE

A GUIDE

Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification, and Training

Prepared by the Cyber Range Project Team and the NICE Community Coordinating Council, Cybersecurity Skills Competitions Community of Interest

September 2023

Applied Information Assurance

Cybersecurity, Forensics, and Incident Response Track (CyFIR)

CyFIR Philosophy

Combine knowledge building and skill building to create a baseline, then allow students to explore and build their experience in a safe environment.

Knowledge Building
Lectures, readings, assignments

Skill Building
Hands-on labs

Experience Building
Group projects (lab building, investigations, research)

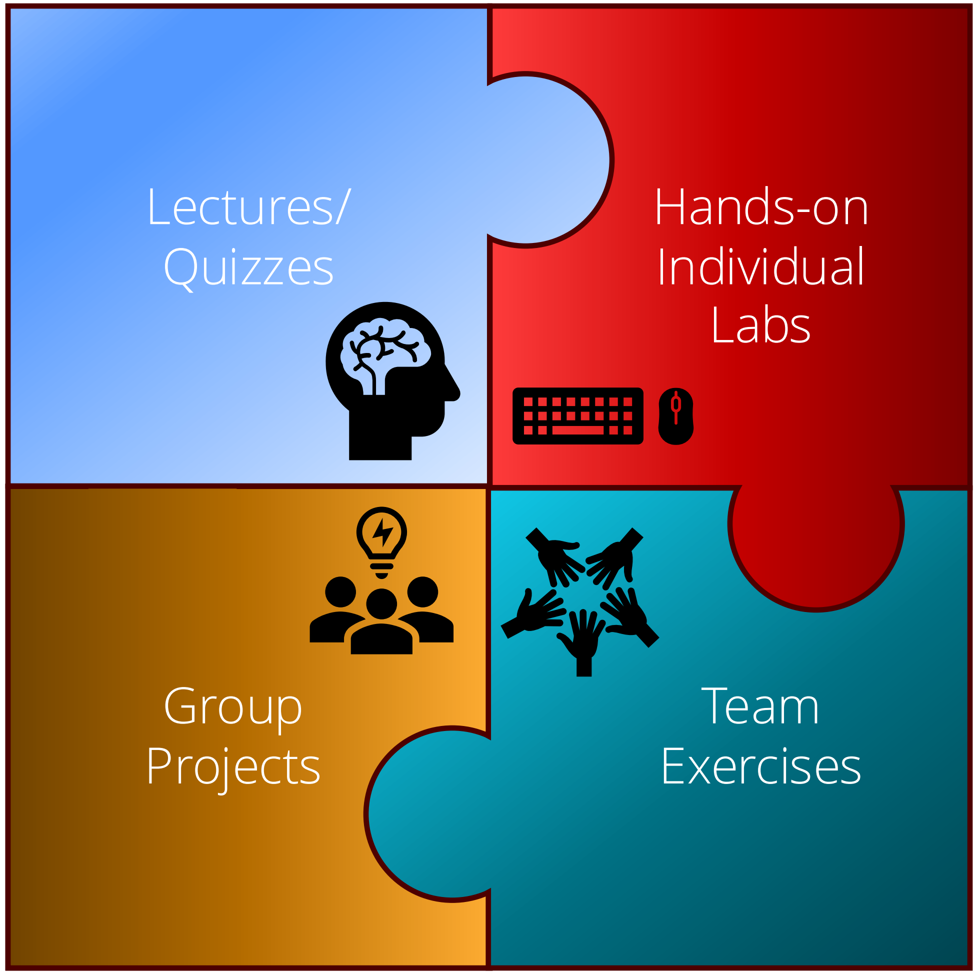
INI 14-761: Applied Information Assurance

Teach and reinforce information assurance and cybersecurity concepts through weekly hands-on labs and group exercises:

- Hacking/Cyber Attacks
- Data Security/Encryption
- Host Security
- Network Security
- Monitoring and Logging
- Introductory Forensics/Incident Response
- Advanced Forensics and Special Topics
- Cloud Security

andrew.cmu.edu/course/14-761

Course Structure



Lectures/ Quizzes

Hands-on Individual Labs

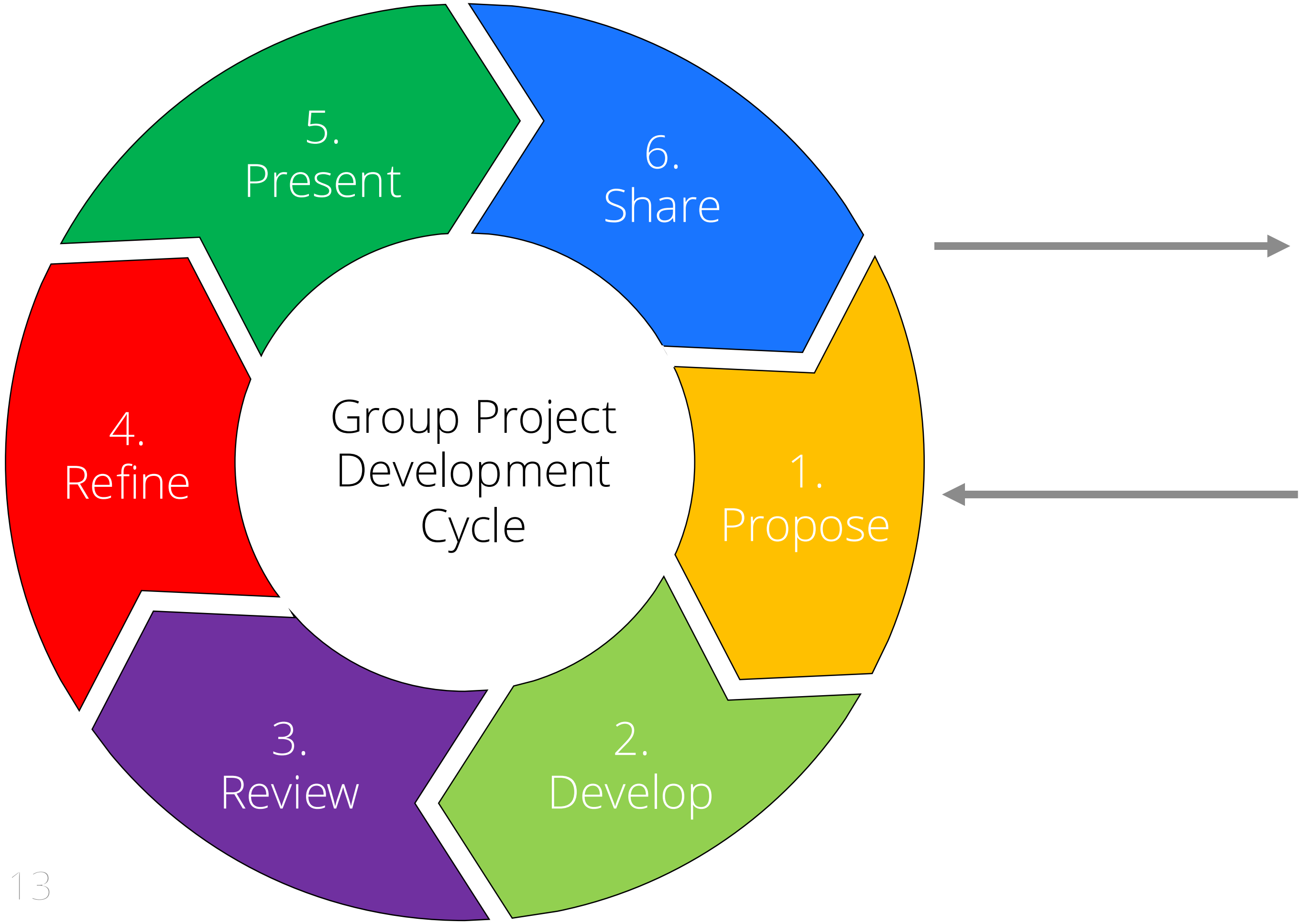
Group Projects

Team Exercises

“Everyone Teaches in AIA”

Alleviates instructor fatigue	Fresh ideas and unique perspectives
Real-world experience in creating and presenting teaching content/Resume builders	Every homework assignment is an exemplar of what to strive for

Continuous Instruction



"Leave Your Legacy"

The top labs are added to the following semester's assignment list where/if applicable to the course topic areas

Instructors can inject replacement options for stale content into the proposal stage

Lab Requirements

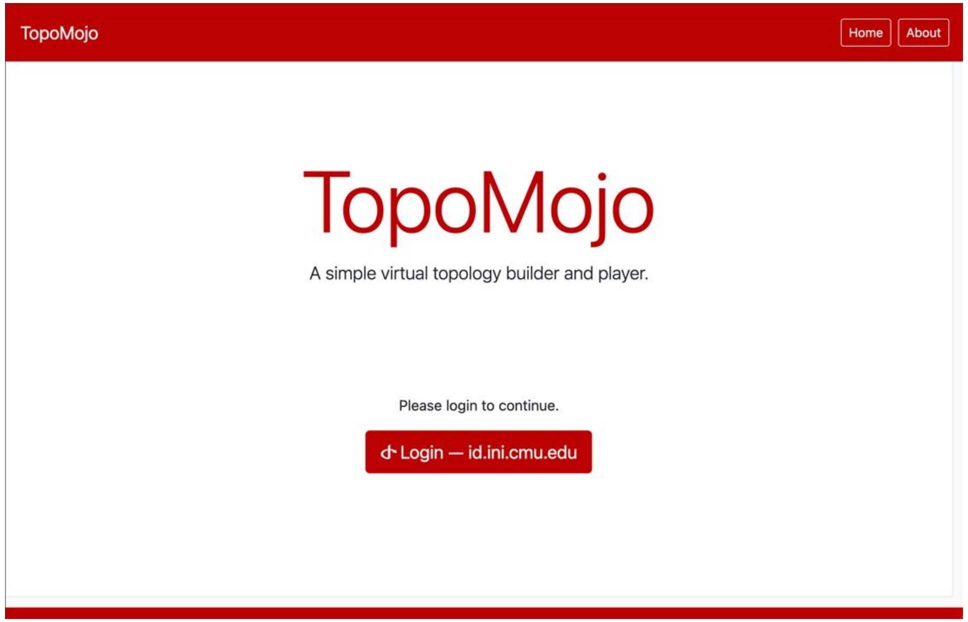
- Learning objectives should be tied back to the topics and concepts taught during class and emphasized in individual and group homework assignments
- Labs include at least five grading scripts or checks to validate the correct state and perform knowledge checks
- Lab instructions should be sound, have a logical flow, be free of errors, and explain the topic well

TopoMojo

Carnegie Mellon University
Information Networking Institute

TopoMojo's Purpose

Make hands-on content development available to *anyone*.



TopoMojo

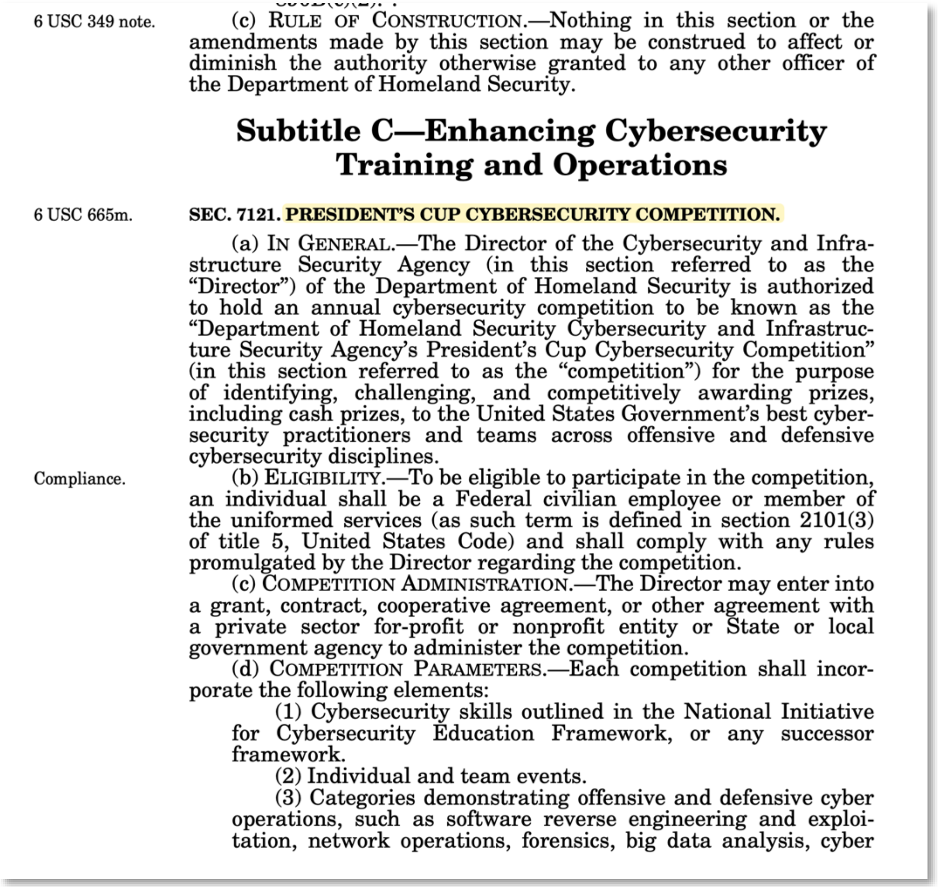
A simple virtual topology builder and player.

Please login to continue.

TopoMojo History

- Developed to allow content creators and trainers to develop their own hands-on cyber labs and exercises.
- Grew in use with the *President's Cup Cybersecurity Competition*, a competition managed by CISA to reward the best cyber practitioners in the U.S. Government.
- Part of SEI's open-source Crucible platform:

cmu-sei.github.io/crucible



6 USC 349 note. (c) RULE OF CONSTRUCTION.—Nothing in this section or the amendments made by this section may be construed to affect or diminish the authority otherwise granted to any other officer of the Department of Homeland Security.

Subtitle C—Enhancing Cybersecurity Training and Operations

6 USC 665m. **SEC. 7121. PRESIDENT'S CUP CYBERSECURITY COMPETITION.**

(a) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency (in this section referred to as the "Director") of the Department of Homeland Security is authorized to hold an annual cybersecurity competition to be known as the "Department of Homeland Security Cybersecurity and Infrastructure Security Agency's President's Cup Cybersecurity Competition" (in this section referred to as the "competition") for the purpose of identifying, challenging, and competitively awarding prizes, including cash prizes, to the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines.

Compliance. (b) ELIGIBILITY.—To be eligible to participate in the competition, an individual shall be a Federal civilian employee or member of the uniformed services (as such term is defined in section 2101(3) of title 5, United States Code) and shall comply with any rules promulgated by the Director regarding the competition.

(c) COMPETITION ADMINISTRATION.—The Director may enter into a grant, contract, cooperative agreement, or other agreement with a private sector for-profit or nonprofit entity or State or local government agency to administer the competition.

(d) COMPETITION PARAMETERS.—Each competition shall incorporate the following elements:

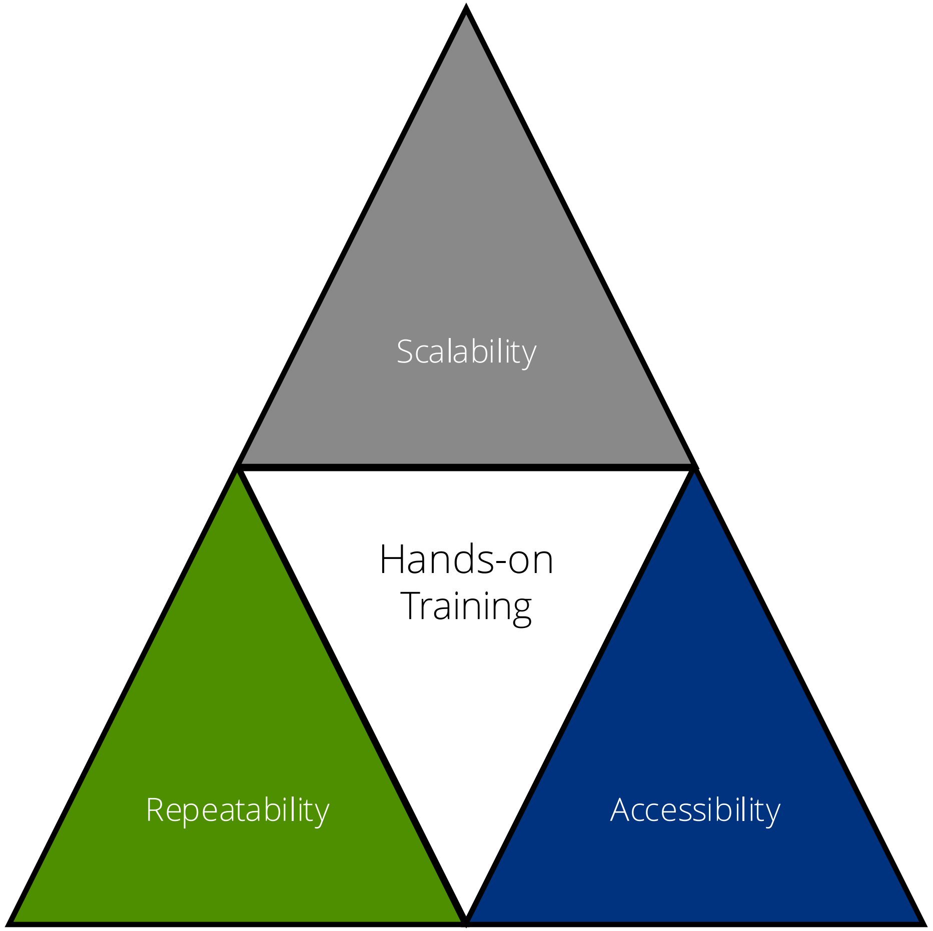
(1) Cybersecurity skills outlined in the National Initiative for Cybersecurity Education Framework, or any successor framework.

(2) Individual and team events.

(3) Categories demonstrating offensive and defensive cyber operations, such as software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber

H.R.7776 - James M. Inhofe National Defense Authorization Act for Fiscal Year 2023

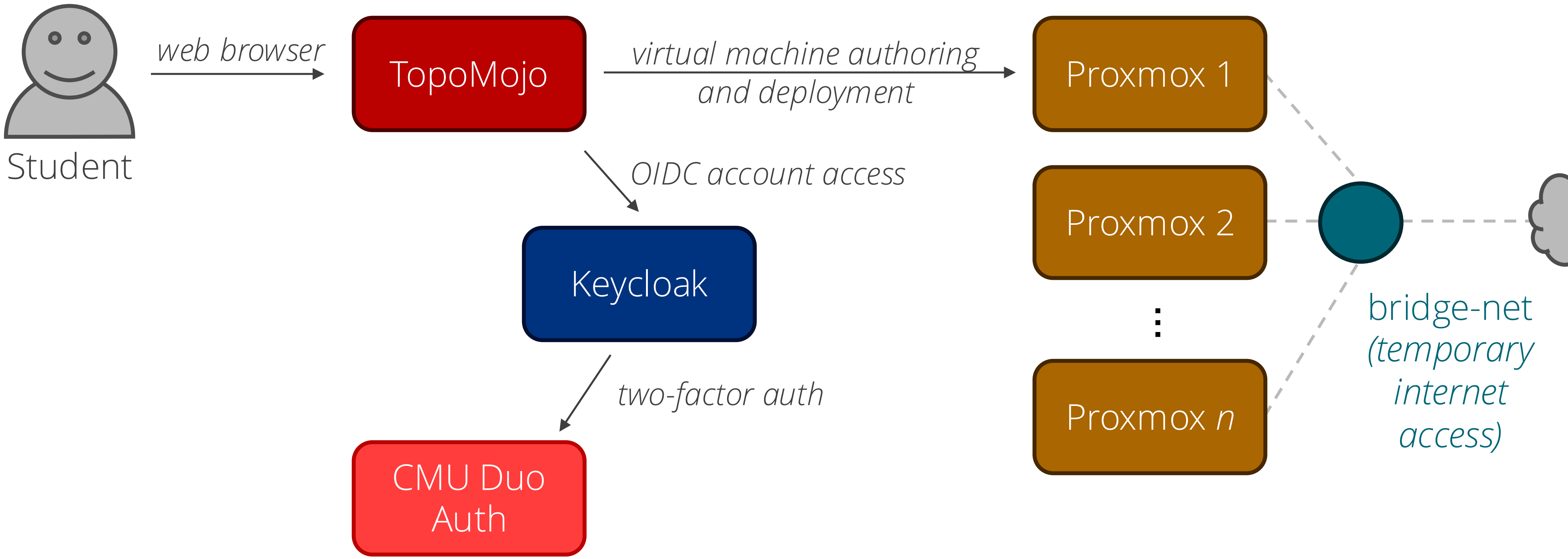
TopoMojo Affordances



TopoMojo Terminology

- Template – Virtual machine starting point
- Workspace – Collection of templates coupled with a lab document authored in Markdown
- Gamespace – Instance of a workspace deployed by a TopoMojo user

TopoMojo Architecture



Lab Authoring Demo

Carnegie Mellon University
Information Networking Institute

Behind the Scenes

CyFIR Infrastructure

Backend Architecture

Diagram TBD

Open Source

Carnegie Mellon University
Information Networking Institute

Upcoming Work

1. **Oasis Cyber Content Library.** Play (and customize) President's Cup competition challenges as TopoMojo labs.

2. **Deployment Automation.** Improve SEI software integration with Proxmox hypervisor. Supports cloud and on-premises deployments for short events or persistent environments.

3. **Community Collaboration.** Engage with other hands-on cyber instructors to find cost-effective ways to improve student experiences

Open-Source Software

- TopoMojo (API)
  github.com/cmu-sei/topomojo
- TopoMojo UI
  github.com/cmu-sei/topomojo-ui
- Foundry Appliance (batteries-included VM)
  github.com/cmu-sei/foundry-appliance
- Test Drive @ NICECyberCon →

niceconference.ini.cmu.edu

Questions?

Carnegie Mellon University
Information Networking Institute

Thank you.

CONNECT WITH US:

Chris Herr
cherr2@andrew.cmu.edu

Matt Kaar
mkaar@cmu.edu

Backup Slides

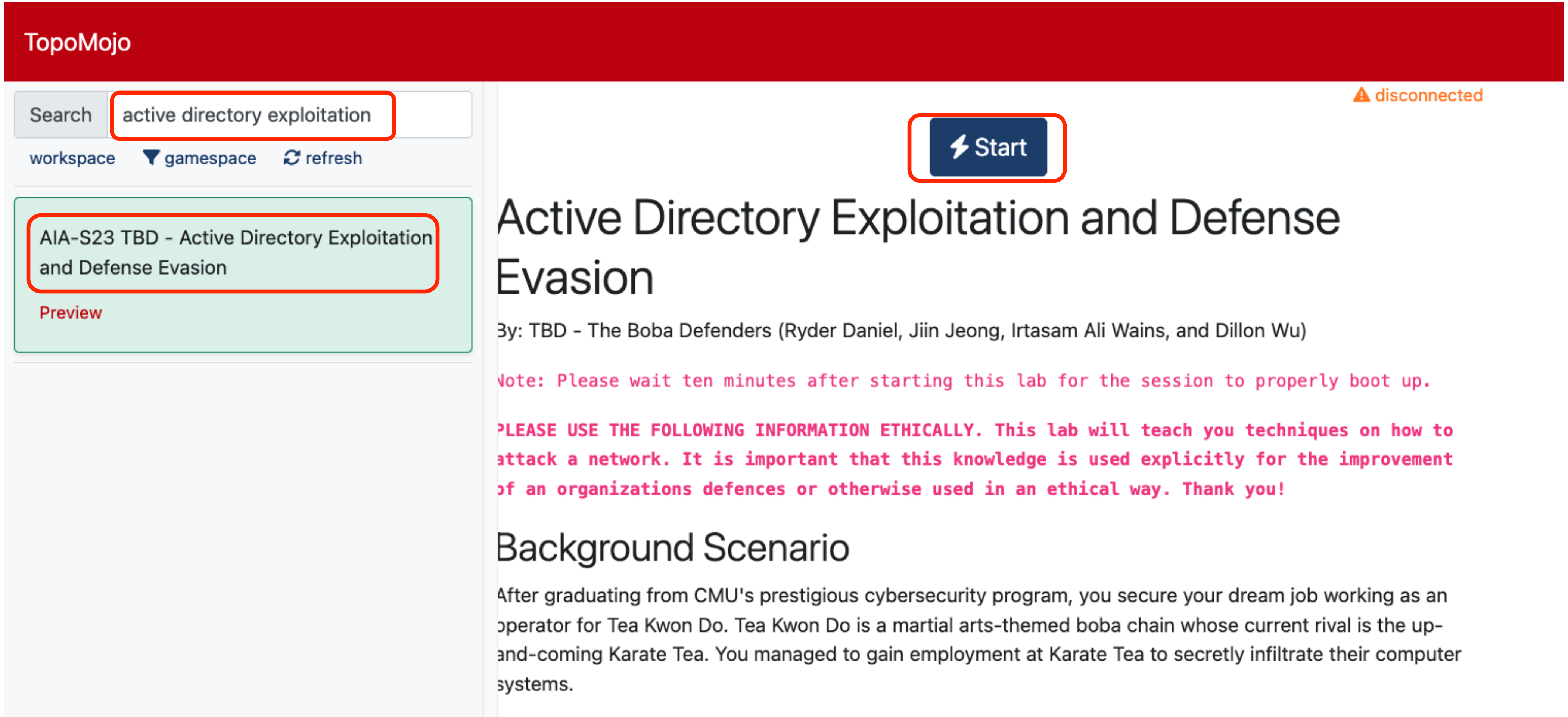
Non-bordered template

The INI was founded in 1989 in response to an industry need to forge collaboration between computer scientists and communications engineers.

Template Slide

- Bullet

Launching a Lab



AIA-S23 TBD - Active Directory Exploitation and Defense Evasion

Active Directory Exploitation and Defense Evasion

3y: TBD - The Boba Defenders (Ryder Daniel, Jiin Jeong, Irtasam Ali Wains, and Dillon Wu)

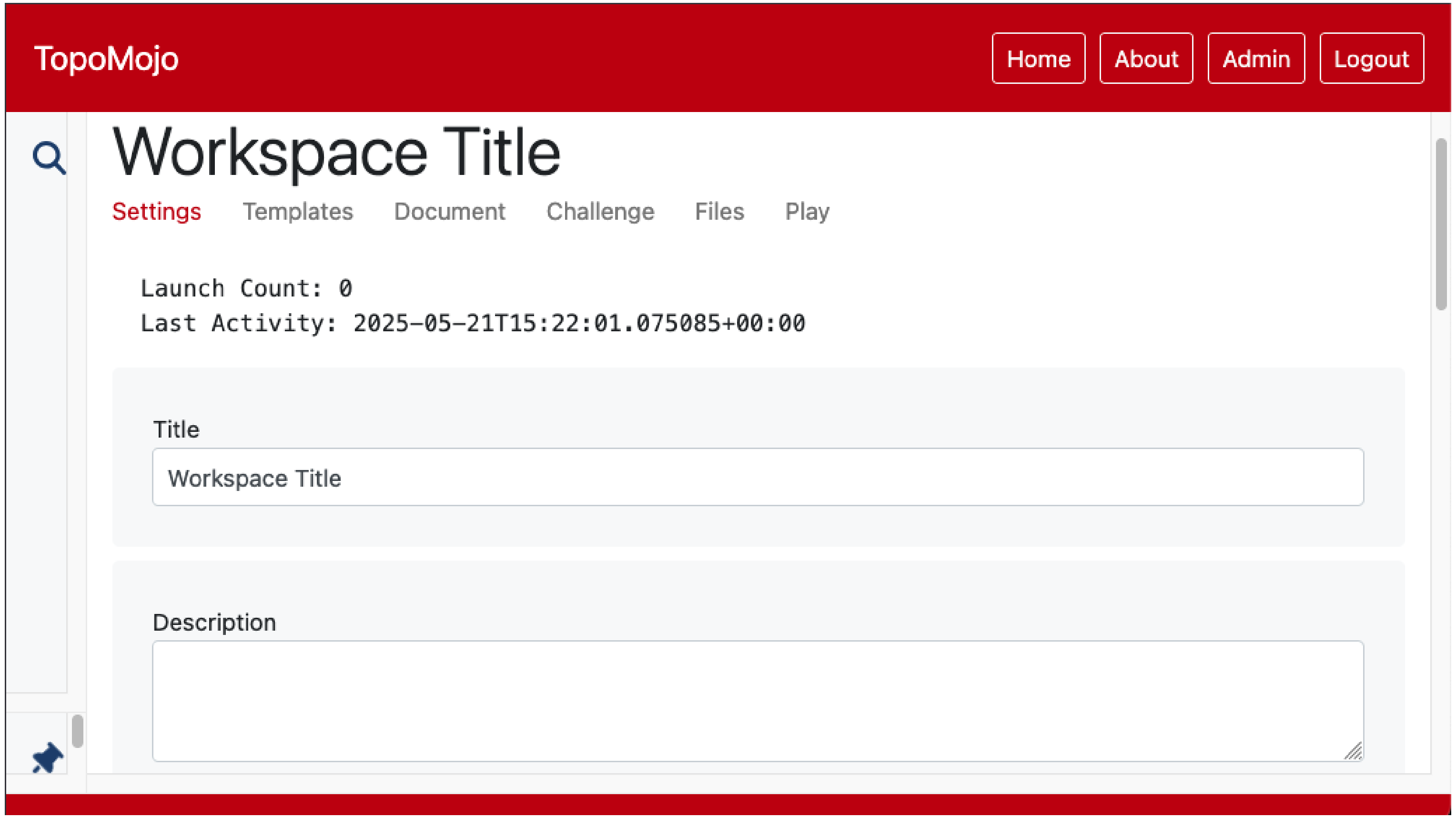
`Note: Please wait ten minutes after starting this lab for the session to properly boot up.`

`PLEASE USE THE FOLLOWING INFORMATION ETHICALLY. This lab will teach you techniques on how to attack a network. It is important that this knowledge is used explicitly for the improvement of an organizations defences or otherwise used in an ethical way. Thank you!`

Background Scenario

After graduating from CMU's prestigious cybersecurity program, you secure your dream job working as an operator for Tea Kwon Do. Tea Kwon Do is a martial arts-themed boba chain whose current rival is the up-and-coming Karate Tea. You managed to gain employment at Karate Tea to secretly infiltrate their computer systems.

Authoring Process



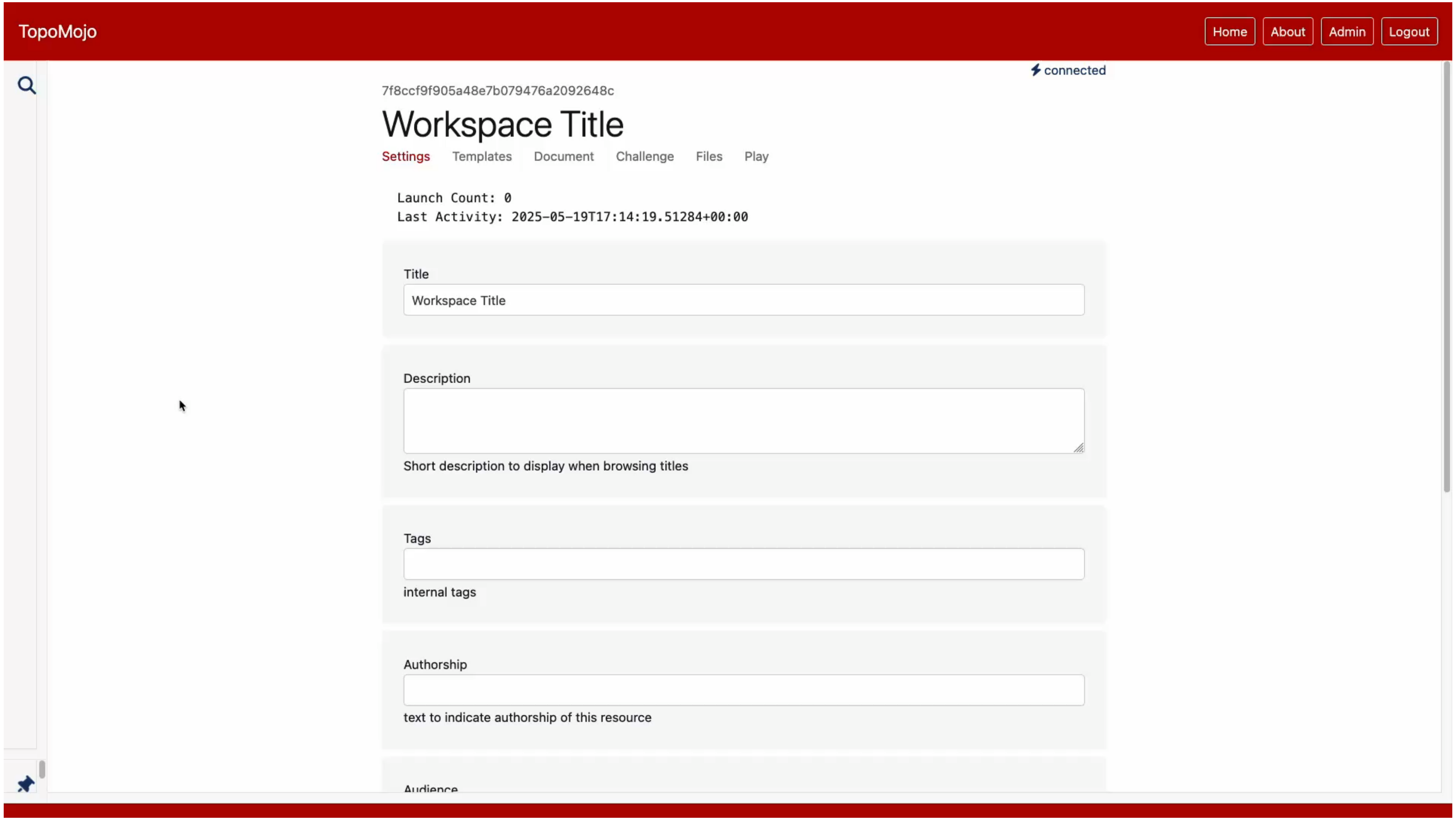
Workspace Title

```
Launch Count: 0
Last Activity: 2025-05-21T15:22:01.075085+00:00
```

Title: Workspace Title

Description:

Authoring Demonstration



7f8ccf9f905a48e7b079476a2092648c

Workspace Title

```
Launch Count: 0
Last Activity: 2025-05-19T17:14:19.51284+00:00
```

Title

Workspace Title

Description

Short description to display when browsing titles

Tags

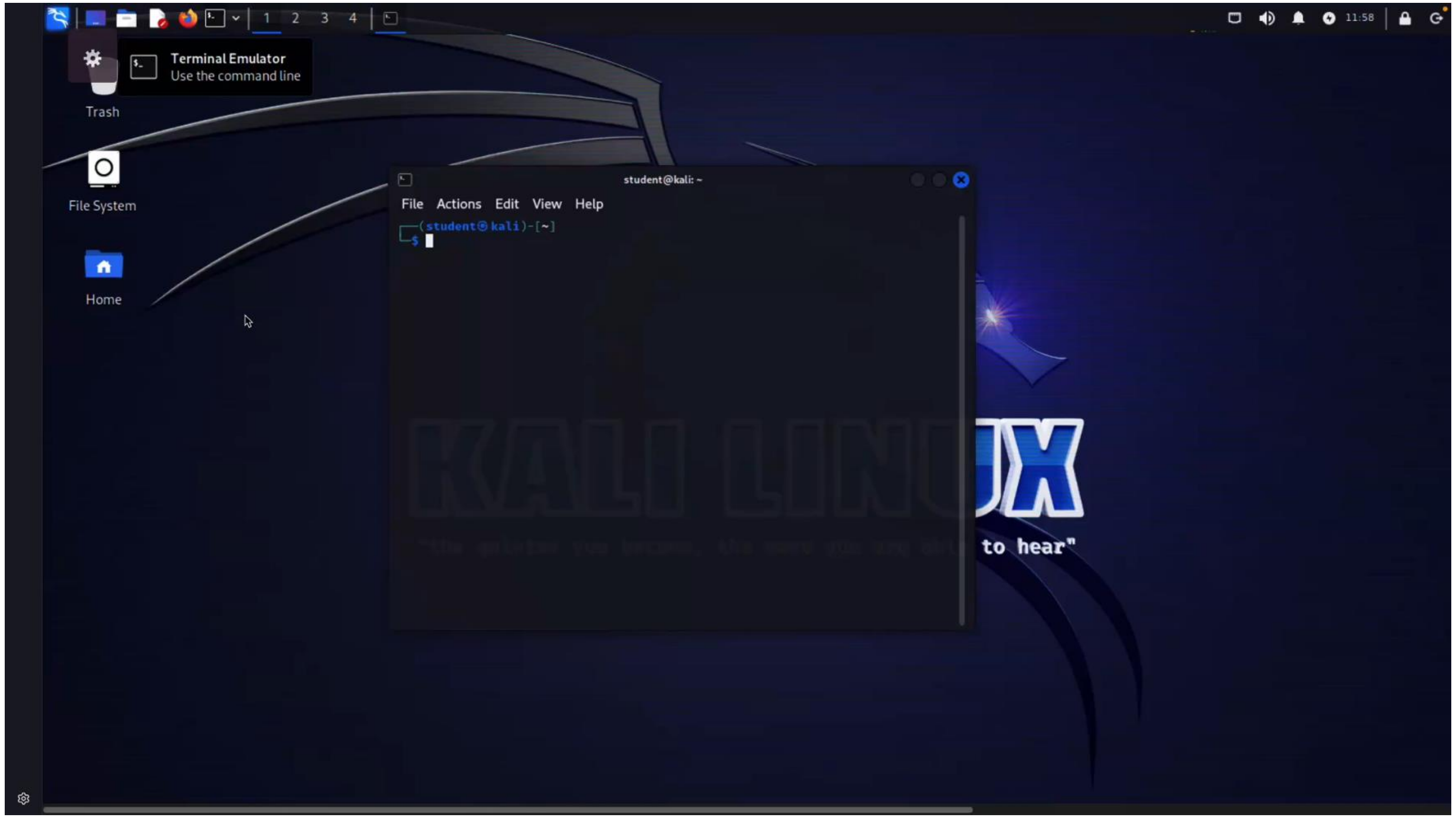
internal tags

Authorship

text to indicate authorship of this resource

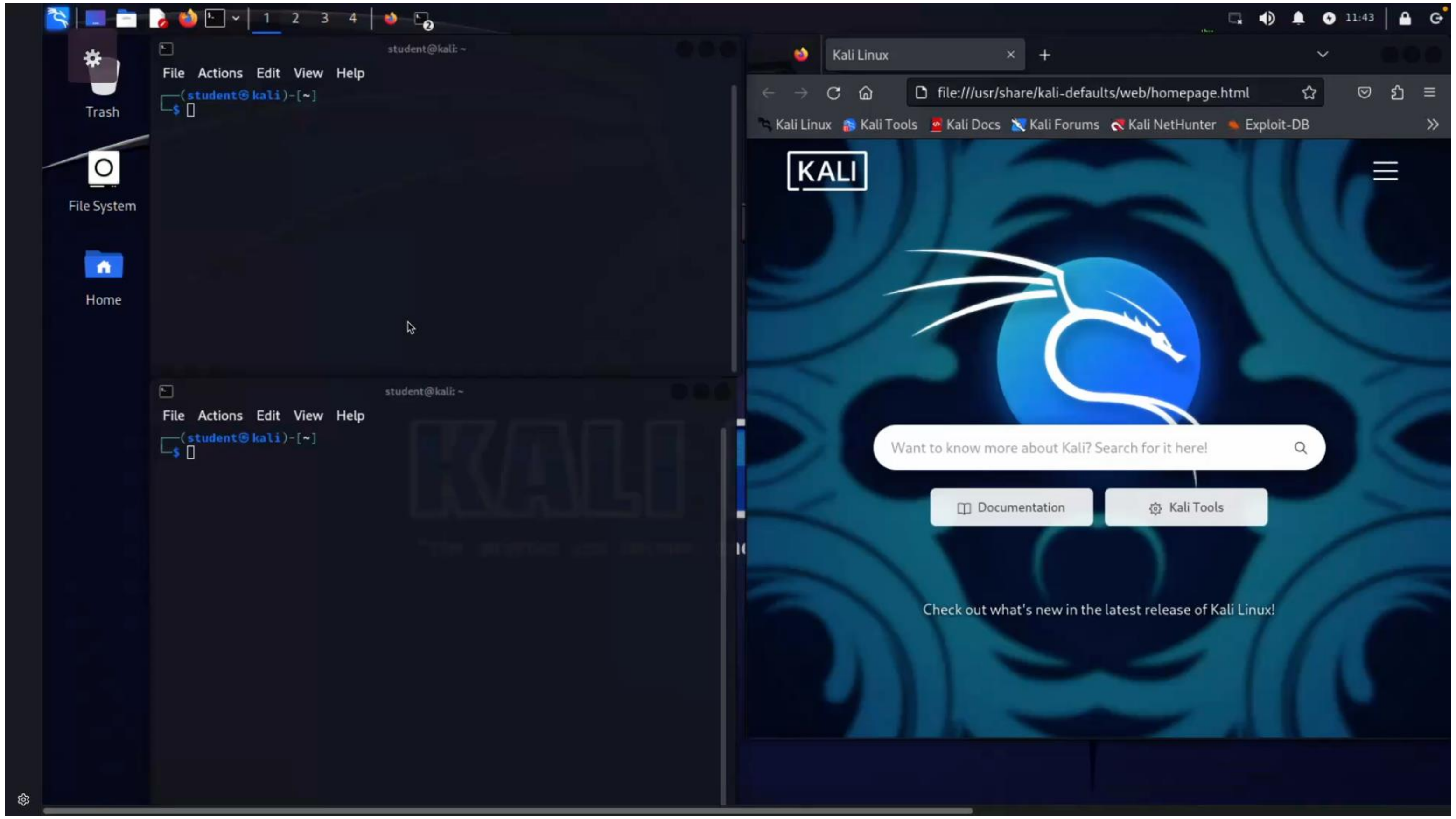
Audience

Copy/Paste



```
┌──(student㉿kali)-[~]
└─$ 
```

Bridgenet (Internet Access)



```
student@kali: ~
┌──(student㉿kali)-[~]
└─$ 
```

```
student@kali: ~
┌──(student㉿kali)-[~]
└─$ 
```

file:///usr/share/kali-defaults/web/homepage.html

Want to know more about Kali? Search for it here!

Check out what's new in the latest release of Kali Linux!