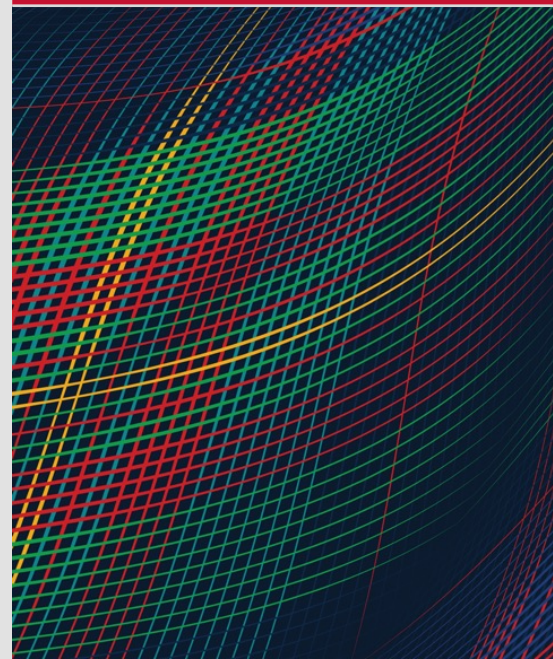


Mission to Mars: Using Video Games to Motivate and Train your Cyber Workforce

Chris May
Jonathan Frederick



Copyright 2023 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.

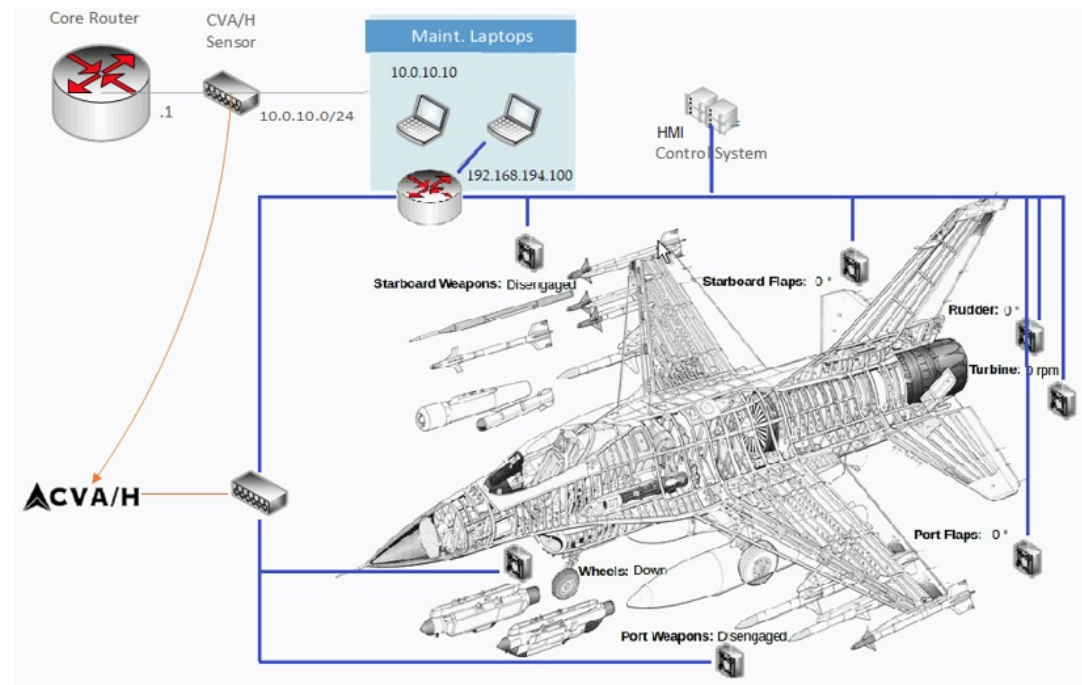
This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

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

DM23-0141

Agenda

- Who We Are
- Why Gaming?
- President's Cup Competition Overview
- Cubespace Game/Demo
- Resources for USAF



Carnegie Mellon University (CMU)

Pioneering discoveries on a global scale



Leading-edge, global research university turning disruptive ideas into successes

2022-2023 *U.S. News and World Report* rankings:

- #1 in artificial intelligence, computer engineering, cybersecurity, management information systems, mobile/web applications, programming languages, software engineering, and quantitative analysis
- #1 in overall computer science

Creating inspired and inventive solutions through sponsored research, faculty and student engagement, executive education, licensing and tech transfer, start ups, and colocation

CMU SEI is a DoD Federally Funded Research and Development Center (FFRDC)



Established in 1984 at Carnegie Mellon University

Charged to improve the state of the practice of **Software Engineering**, **Cybersecurity**, and **Artificial Intelligence**

Collaborates with CMU and broadly in academia, government, and industry

Capable of conducting both fundamental research and classified work

~650 staff members

Offices in Pittsburgh and DC, with locations near customer facilities

CERT Division – Birthplace of Cybersecurity Research



1988

Computer Emergency Response Team formed in response to the Morris Worm

2022

Cybersecurity Engineering and Resilience Team conducting collaborative and innovative evidence-based research to fortify the cyber ecosystem and protect national security and prosperity

Trusted

Conducting research for the U.S. Government in a non-profit, public-private partnership

Valued

Innovating solutions with a global collaboration of military, industry, and academia

Relevant

Achieving results for our mission partners

Who are these guys?

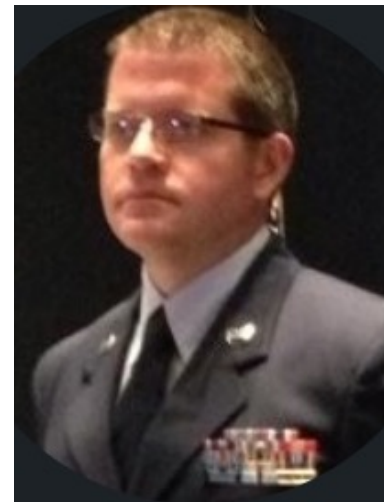
Chris May

- Technical Director at CMU/SEI
 - Cyber Mission Readiness
- Former USAF Comm Officer
- First OTS class at Maxwell Sep '93



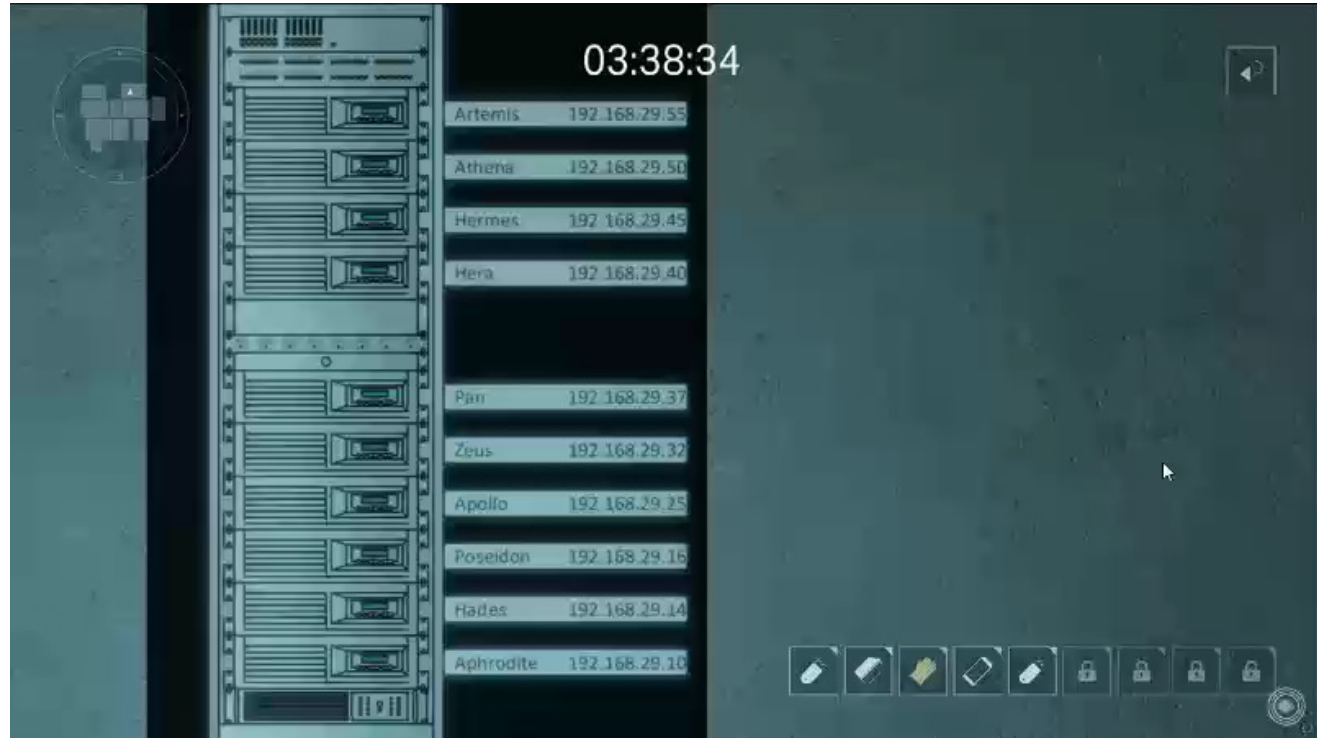
Jonathan Frederick

- Senior Cybersecurity Engineer at CMU/SEI
 - Cyber Mission Readiness
- Retired USAF/ANG Cyber NCO
- Leads President's Cup; PhD student



Why Gaming? Does it work for Cyber Training? Yup!

- Motivation; play and learn after hours
- Attention and Retention
- Collaborative; designed to encourage/require teamwork
- Works as curriculum framework; level up for next block of training



Why Gaming? What the research says...

- “Introducing the game in the educational curricula improves student engagement and consolidates their knowledge on cybersecurity.” (Ros, S., et. al, 2020)
- “Our analysis shows that ... gamification ... has increased the effectiveness of self-learning and motivation as well as helped to improve the median grade of students” (Demmese, F., et. al, 2020)



President's Cup Cybersecurity Competition Overview



- Presidential Executive Order 13870; codified into law via FY23 NDAA
- Identify & reward top cyber talent in federal government
- Thousands of participants from DoD and federal civilian departments & agencies
- Challenges and solution guides available after each competition
- Platform has been open sourced

President's Cup Challenges

NICE Framework Work Roles



INDIVIDUAL COMPETITION

There are two tracks available within the Individuals competition. Individuals can choose to participate in one or both tracks based on their interest.

TRACK A

PRIMARY	Cyber Defense Incident Responder
	Cyber Defense Forensics Analyst
SECONDARY	Network Operations Specialist
	Cyber Defense Analyst

TRACK B

PRIMARY	Exploitation Analyst
	Cyber Operator
SECONDARY	Research & Development Specialist
	Vulnerability Assessment Analyst



TEAMS COMPETITION



The 2022 President's Cup Team Competition will consist of tasks drawn from the following eight in-demand NICE Framework roles:

TEAMS:

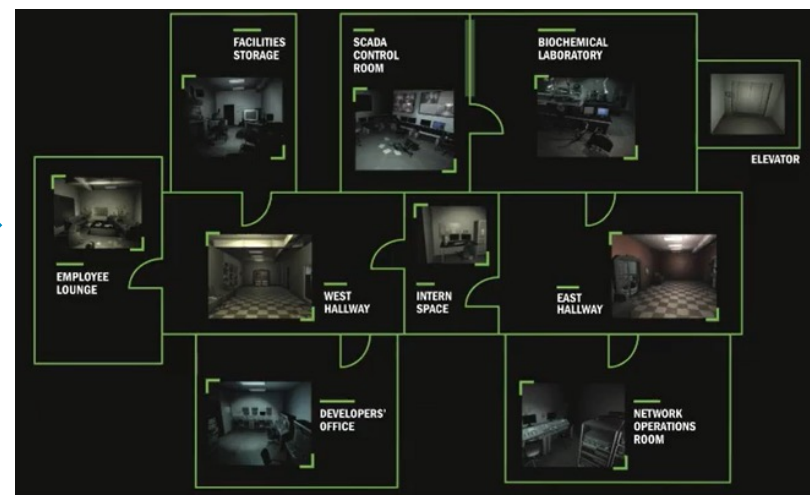
Cyber Defense Incident Responder	Exploitation Analyst
Cyber Defense Forensics Analyst	Vulnerability Assessment Analyst
Network Operations Specialist	Data Analyst
Cyber Defense Analyst	Threat/Warning Analyst

President's Cup Finals

2019 – Escape Room



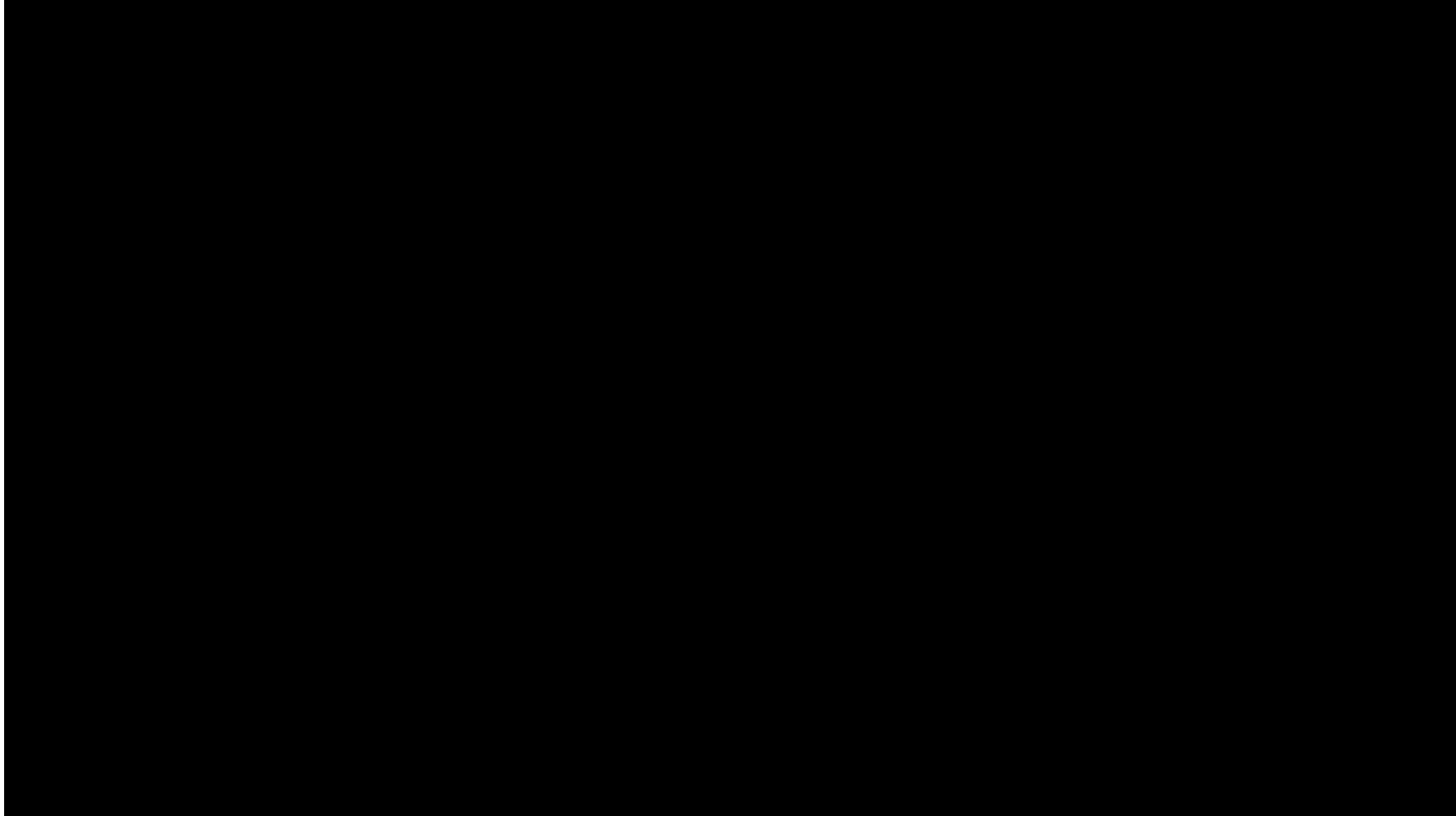
2021 – Alien Threat



2020 – Winter Superstorm Recovery



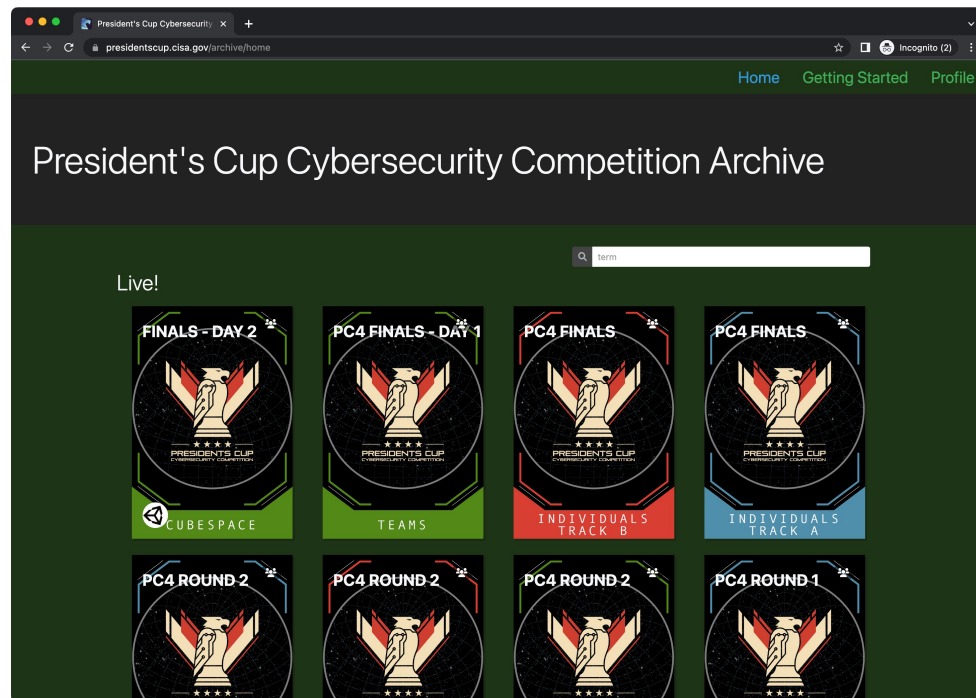
Cubespace Game Scenario – The Storyline is Crucial



Cubespace Game Play – User Interface must be Intuitive



Archive Site for Training – Builds Hands-on Skills



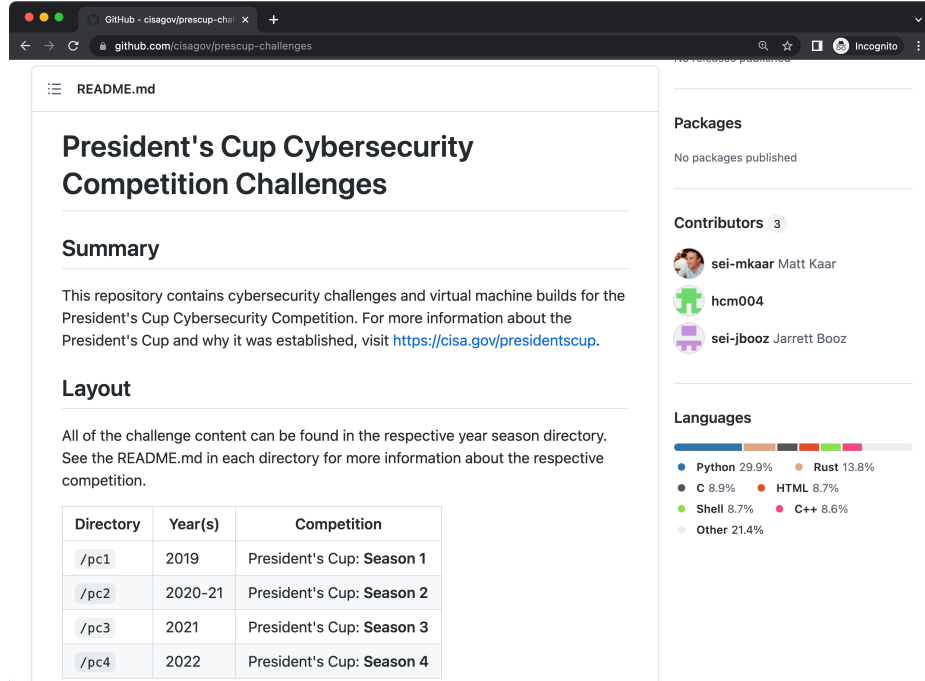
The **President's Cup Competition Archive** hosts > 150 live challenges from Seasons 2-4 (2020-2022).

Registration open to anyone with a **.mil or .gov email address**.

Includes most recent President's Cup Finals video game, Cubespace. Playing this as a team is highly encouraged.

presidentscup.cisa.gov/archive

Open-Source Challenges & Solution Guides



The screenshot shows the GitHub repository page for 'cisagov/prescup-challenges'. The main content area displays the README.md file, which includes the title 'President's Cup Cybersecurity Competition Challenges', a summary, and a layout section. The layout section states that all challenge content can be found in the respective year season directory and provides a table of directories. The table has three columns: Directory, Year(s), and Competition. The right sidebar shows the repository's statistics, including no published packages, three contributors (sei-mkaar, hcm004, and sei-jbooz), and a language distribution chart.

President's Cup Cybersecurity Competition Challenges

Summary

This repository contains cybersecurity challenges and virtual machine builds for the President's Cup Cybersecurity Competition. For more information about the President's Cup and why it was established, visit <https://cisa.gov/presidentscup>.

Layout

All of the challenge content can be found in the respective year season directory. See the README.md in each directory for more information about the respective competition.

Directory	Year(s)	Competition
/pc1	2019	President's Cup: Season 1
/pc2	2020-21	President's Cup: Season 2
/pc3	2021	President's Cup: Season 3
/pc4	2022	President's Cup: Season 4

Languages

- Python 29.9%
- Rust 13.8%
- C 8.9%
- HTML 8.7%
- Shell 8.7%
- C++ 8.6%
- Other 21.4%

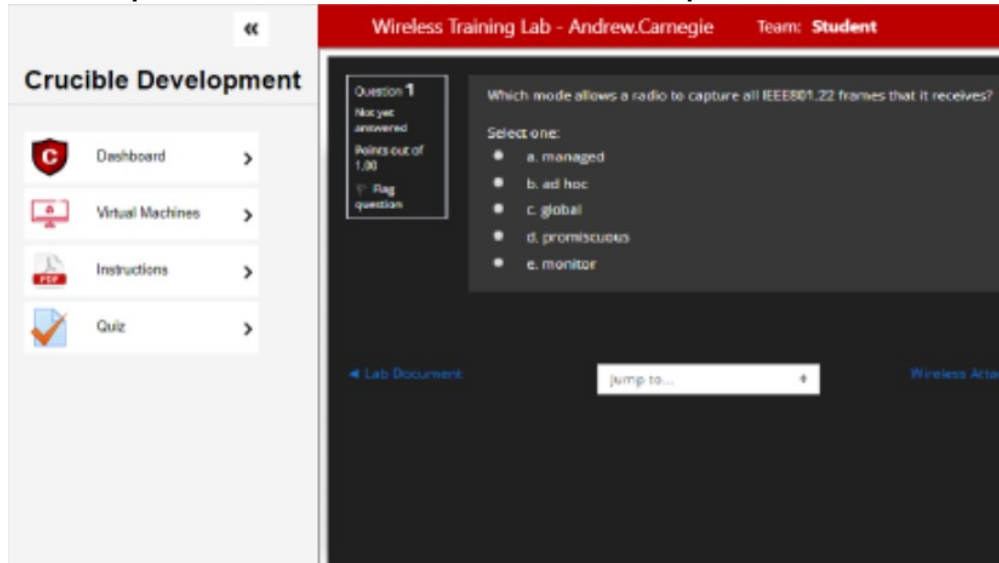
Documentation, artifacts and solution guides are available for past President's Cup challenges on CISA's GitHub site.

This repository serves to educate future competitors and provide resources for cybersecurity training.

github.com/cisagov/prescup-challenges

Crucible

- Open-source cyber range/simulation framework
- In use by 318/RANS, 39/IOS plus USSOCOM and USINDOPACOM
- “Infrastructure as code” for topology building
- On-prem and cloud virtualization platforms



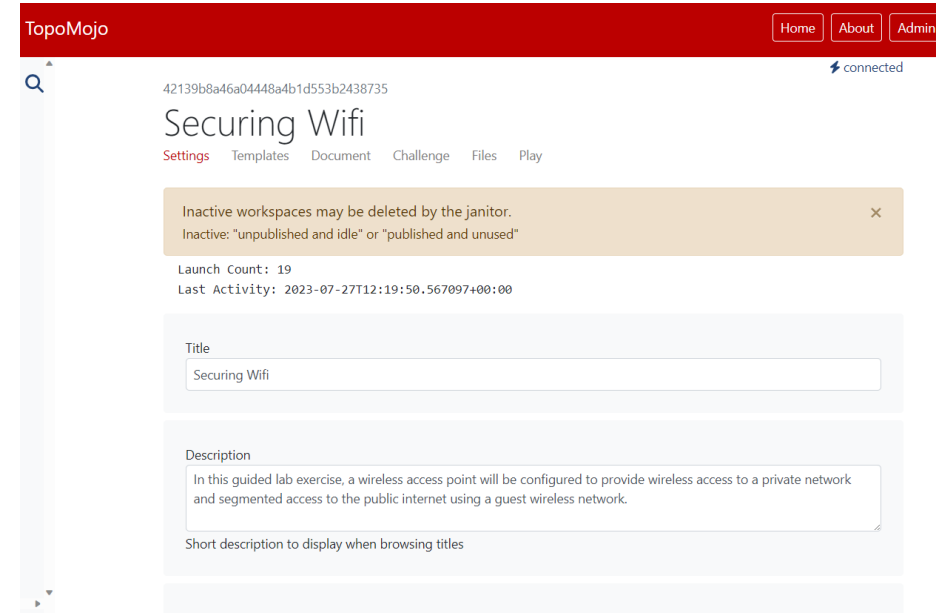
<https://cmu-sei.github.io/crucible/>

<https://github.com/cmu-sei/crucible>

Mission to Mars: Using Video Games to Motivate and Train your Cyber Workforce
© 2023 Carnegie Mellon University

Foundry Appliance

- Open-source Cyber competition and simplified training platform
- In use by DHS/CISA, and several .edu's



<https://cmu-sei.github.io/foundry-docs/>

<https://github.com/cmu-sei/foundry-appliance>

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Conclusion

- Video games can be a powerful vehicle for cybersecurity training
- Research shows improved learning outcomes; greater retention
- Motivates students to work together and even after hours
- Open-source game, platforms, and content available for widespread use
 - .gov/.mil can access content on CISA's platform: <https://presidentscup.cisa.gov>



Questions?

Chris May - cjm@cert.org
Jonathan Frederick - jjf205@cert.org