



PPS{CYBERTACTICSFEST}

Harnessing Competition to
Drive Deep Understanding

link to slides



[https://tinyurl.com/
ppsCTF-edcon25-pres](https://tinyurl.com/ppsCTF-edcon25-pres)

objectives

express an interest



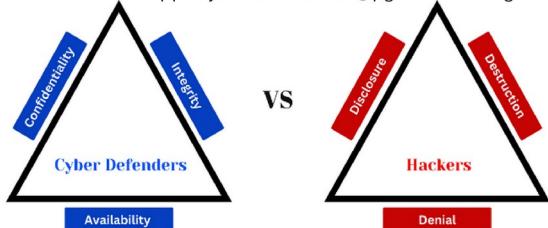
objectives

-  utilize the competitive spirit of adolescence to increase exploration and innovation
-  provide tools and skill-focused content to ensure that lessons were actionable
-  reduce barriers to entry by explicitly teaching every skill to be used in the competition
-  connect students to a community of like-minded peers where they could be recognized for their skills and efforts

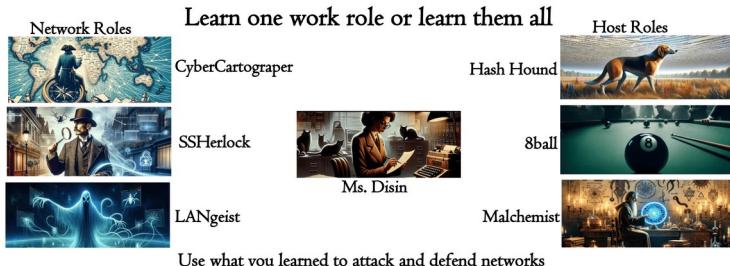
how it begins

pps{CyberTacticsFest}

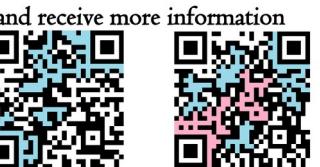
ppsCyberTacticsFest@pghschools.org



The PPS Cyber Tactics Fest aims to immerse students in realistic cybersecurity scenarios. Aligning with the MITRE ATT&CK framework and leveraging skills aligned with Carnegie Mellon University's PicoCTF and Cyber.org, this unique version of adversarial CTF will give real-world and hands-on skills with the incentives that only competition and gamification can provide.



Accept one of these challenges to show an interest in participating



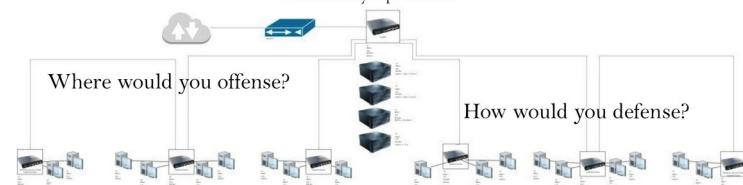
tinyurl.com/nscctf-invite-base

tinyurl.com/psecctf-invite-sherlock

tinyurl.com/psecctf-invite-betwixt

Season starts second semester 1-2 sessions per week, individual and team challenges, culminating tournament

Whether you want cybersecurity as a career, a position to help work through college, or want to learn how hackers think, this competition will give you the tools, methods, and mindset to compete in a field that touches every aspect of life.



how it begins - students

invites sent to former
students/participants

posters placed in high schools

5x7 challenge cards placed
strategically



[Tinyurl.com/ppsctf-invite-base](http://tinyurl.com/ppsctf-invite-base)

[Tinyurl.com/ppsctf-invite-sherlock](http://tinyurl.com/ppsctf-invite-sherlock)

[Tinyurl.com/ppsctf-invite-betwixt](http://tinyurl.com/ppsctf-invite-betwixt)

[Tinyurl.com/ppsctf-invite-mise](http://tinyurl.com/ppsctf-invite-mise)

how it begins -students

simple ctfs with hints on the page

to submit the flag, you submit a
form that expresses interest

a total of 52 students submitted
flags and were invited to join a
team

how it begins - staff/admin

Invitation to Engage in pps{CyberTacticsFest}

- Cybersecurity Coaching, Mentorship, Development Program-

We enthusiastically invite you to help support the pps{CyberTacticsFest}, an initiative to introduce cybersecurity education in Pittsburgh Public Schools. Your role is not only crucial for nurturing upcoming talents but serves as an opportunity for you to expand your expertise, develop leadership skills, apply your insights, and make a substantial impact in the field.

As a broad overview of the season and competition: The competition environment consists of 16 Kali VMs (student boxes) and 20-26 ZorinOS VMs (target boxes). The competition itself is an offensive/defensive capture the flag in which teams of 8 are simultaneously capturing flags the other teams 10-13 target boxes while defending flags on their own. All the flags are directly tied to skills presented and housed on the competition SharePoint.

To prepare for the competition, MS Teams meetings are held 7-9pm Tuesday and Thursday evenings starting in February. These "combined" practices utilize the cyber.org range to present the skills needed to be successful in the competition or present the opportunity for students apply the skills in mini-challenges that combine skills recently presented. Towards the end of the season, whole team challenges are presented to allow teams to develop their collective skills.

You are invited to participate in the following ways: A coach, mentor, or developer.

As a coach you will be attached to a team of 4-8 students who are expected to learn 1-4 'work roles' each. You, and potentially a co-coach, will be given access to the cyber.org range to hold practices outside of the normal presentation times. Practices times will be up to you and your team. Those with PA child abuse clearances will have the freedom to host practices at any time, those who do not have clearances need to coordinate with PPS staff to ensure that someone with clearances will be in the virtual meeting. The content of the practices can be as simple as a review of the concepts and skills taught in the combined practice or a practical exercise for the team. The combined practices tend to lack the repetitions needed to develop skills, however, the content of the practices is by and large left up to the coaches.

As a mentor, you will be attached to a single 'work role' and the skills associated with it. You will assist in the application and integration of that work role more vertically by helping develop the location of flags in the final competition, the small-team challenges associated with that work role, the practical exercises associated with the work role on the SharePoint (can be linked directly to picoCFT) and the presentation of that work role during combined practices. The level and time commitment of the mentors is more based upon the task. They will be given access to the Cyber.org range (picoCTF is whitelisted on the Kali) to ensure practical exercises developed are feasible, the pps{CyberTacticsFest} SharePoint to advise on content, as well as the template for the target machines to develop flags for the final competition.

As a developer, you will be assisting in the final competition. The final competition scenario is a fictional school in which something mysterious is happening. Last year's scenarios were Science Teachers as Lizard People Overlords and Track Coaches as Immortal Trojans. Each scenario had 3 layers of boxes at various levels of difficulty for the network teams to get into and 3 'levels' of difficulty for the host teams to capture flags out of. The development of the target machines, and the scenarios that go along with them, requires a broader understanding of how the various skills being taught could manifest as flags in an environment. Alternatively, you may develop additional capabilities to monitor the competition. Some items on the horizon are utilizing CTFd for flag submission, SecOnion for automatic points awarding, a live scoreboard and a live broadcast of SecOnion and Wireshark to share and promote the competition with outside professionals.

Your participation in this initiative would be greatly appreciated as it has outgrown its current level of support. This is a remarkable opportunity to leave a lasting imprint in the cybersecurity education landscape. We earnestly hope you will consider joining us at pps{CyberTacticsFest}. Your expertise, passion, and guidance will be pivotal to our students' success.

Please feel free to reach out to Jacob Boyce at jboyce1@pghschools.org to express your interest or any queries.

Thank you for considering this vital contribution to shaping the future of cybersecurity education.

Warm regards,

Jacob Boyce

invited all staff/admin within 65 miles of PPS

invited CMU, Pitt, ARCPB

invited local cybersecurity firms

invited diversity-focused organizations

A total of 247 invitations sent

how it begins - staff/admin



[https://tinyurl.com/
ppsCTF-gradinvite-25](https://tinyurl.com/ppsCTF-gradinvite-25)

Received volunteers to mentor/coach from:

BlackGirlsHack.org

Carnegie Mellon University picoCTF

US Army CPT 186

Building a community of support for the
program is small and incremental

how we trained

Sections

- pps{CyberTacticsFest} 2024-25 Season
- A nod of respect to those who have helped this process

pps{CyberTacticsFest} 2024-25

Season

Schedule of Events

2/4 Tuesday 7-9pm Teams Meeting: Intro and overview, cyber.org range, big picture scenario, intro to outside resources; picoCTF.

2/6 Thursday 7-9pm Teams Meeting: SSherlock (Network)

2/11 Tuesday 7-9pm Teams Meeting: HashHound (Host)

2/13 Thursday 7-9pm Teams Meeting: Small Team Challenge (based on newly introduced skills)

2/20 Thursday 7-9pm Teams Meeting: CyberCartographer (Network)

2/25 Tuesday 7-9pm Teams Meeting: Ms. Disin (Host)

2/27 Thursday 7-9pm Teams Meeting: Small Team Challenge

3/4 Tuesday 7-9pm Teams Meeting: Q/A Session

3/6 Thursday 7-9pm Teams Meeting: Small Team Challenge Preperation/ Review

3/11 Tuesday 7-9pm Teams Meeting: Small Team Challenge

3/13 Thursday 7-9pm Teams Meeting: LANgeist (Network)

3/18 Tuesday 7-9pm Teams Meeting: MALchemist (Host)

3/20 Thursday 7-9pm Teams Meeting: Small Team Challenge

3/22 Saturday 9am-1pm Live Meeting: 1400 Crucible St. Pittsburgh, PA 15205

3/25 Tuesday 7-9pm Teams Meeting: PortalLord (Network)

3/27 Thursday 7-9pm Teams Meeting: 8ball (Host)

3/29 Saturday 9am-1pm Live Meeting: 1400 Crucible St. Pittsburgh, PA 15205

4/1 Tuesday 7-9pm Teams Meeting: Whole Team Challenge

4/3 Thursday 7-9pm Teams Meeting: Whole Team Challenge Review

4/9 Wednesday 9am-2pm Greenway: Round 1 A (Brashears/CAPADice)

4/10 Thursday 9am-2pm Greenway: Round 1 B (SciTech/ObamaHouse)

4/11 Friday 9am-2pm Greenway: Round 2 A/B

Upcoming Events:

- May-June: Western PA PicoCTF Regional Invitational Competition (Date TBD)

A nod of respect to those who have helped this process

ppsCTF

- SSherlock (Network)
- HashHound (Host)
- CyberCartographer (Network)
- MsDisin (Host)
- LANgeist (Network)
- MALchemist (Host)
- Portalord (Network)
- 8ball (Host)

how we trained

8 "workroles" divided into host and network

participants encouraged to attend meetings and challenges for one host and one network

Tuesday Thursday 7-9pm teams meetings to present workroles

MS Teams meetings allowed for more participation but many students did not feel as engaged online, adjustments being made for next season

how we trained
meet the work-roles:

Network Roles



Cyber-
cartographer



SSherlock



Langeist



Ms. Disin

Host Roles



Hash
Hound

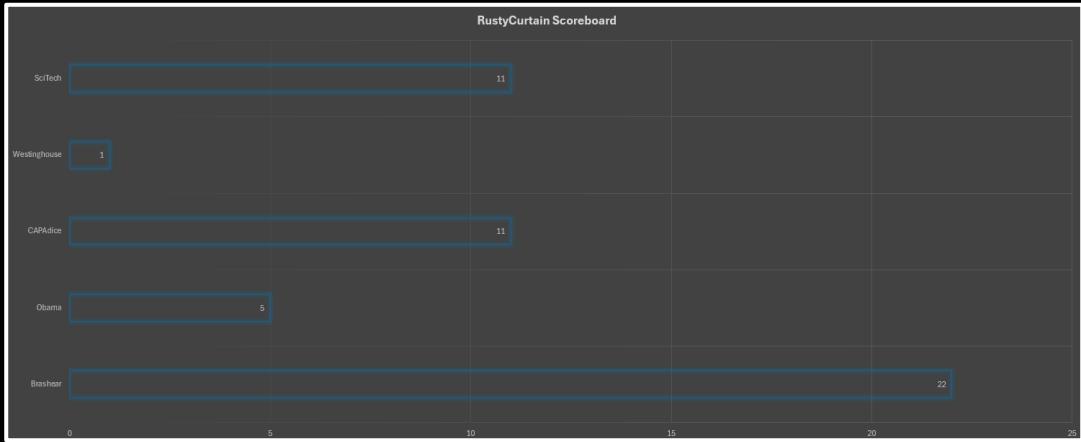


8ball



Mal-
Chemist





ppsCTF / challenges / rustycurtain /

| Name | Last commit message |
|-----------------------------|--|
| ... | |
| boris.zip | Add files via upload |
| challenge_instructions.txt | Update challenge_instructions.txt |
| ctf1.py | Update and rename setup_ctf_cpu1.py to ctf1.py |
| ctf2.py | Create ctf2.py |
| deploy-telnet-23.py | Add files via upload |
| ftp-anon-highport.py | Add files via upload |
| ftp-anon-login.py | Add files via upload |
| ivan.zip | Add files via upload |
| nikoli.zip | Add files via upload |
| rustycurtain-prep-setup.txt | Create rustycurtain-prep-setup.txt |
| ssh-highport-generator.py | Update ssh-highport-generator.py |
| tanya.zip | Add files via upload |
| yuri.zip | Add files via upload |

how we trained
meet the mini-challenges:

CyberBully

HamHunt

RustyCurtain

CornerPocket

Hayloft

ppsCTF / challenges / CornerPocket / instructions

Code **Blame** 64 lines (50 loc) · 1.45 KB

```

23 sudo sed -i 's/^#\?PasswordAuthentication .*/P
24
25
26 Box 2:
27
28 adduser <choose from below>
29
30 stjones8
31 stmiller4
32 stbrown8
33
34 password:
35 Y0uf0undm3B@!
36 P@ssw0rd!
37 Secur1ty!
38 Cha1nL0ck!
39 H@ckM3N0w!
40 Saf3Guard!
41 K33p0ut!
42 Pr0t3ct!
43 F0rtR3ss!
44 Gu@rd1@n!
45 LockD0wn!
46
47 su <user>
48 password <password>
49

```



how we trained meet the mini-challenges:



CyberBully

In the CyberBully challenge, students responded to a hostile digital campaign between two feuding families, where siblings from one side were launching cyberattacks to harass and intimidate the other. Players used Wireshark to analyze network traffic, identify malicious IP addresses, and trace the source of bullying messages hidden in packet captures. As they dug deeper, they uncovered a piece of malware embedded in a shared file that revealed the attackers' plans and network backdoors. Students had to block ports, isolate systems, and launch precision packet-based countermeasures, including TCP resets and memory-level defenses, to protect the victim's systems and expose the perpetrators.



how we trained

meet the mini-challenges:



In the HamHunt challenge, students investigated suspicious transmissions from a ham radio operator convinced he had made contact with extraterrestrials. By pivoting across a family's network of devices—starting with a teenage son's laptop, brute-forcing the mother's credentials, and finally accessing the father's computer—participants uncovered odd logs, encrypted files, and a mismatched hash pointing to a fabricated “alien message.” The challenge emphasized user profiling, SSH exploitation, hash analysis, and adversarial file tracing, blending the SSHerlock and HashHound roles to reconstruct the delusional operator's digital trail.

HamHunt



how we trained

meet the mini-challenges:



In the RUSTyCurtain challenge, students explored a Cold War intelligence leak in which altered texts were injected into public archives to manipulate perceptions of historical events. Working in the roles of Ms. Disinfo and CyberCartographer, they used text comparison tools to uncover embedded disinformation and leveraged file structure and network mapping to trace the origin of tampered documents. Success required identifying inconsistencies across versions, detecting strategic word replacements, and correlating document paths to their points of compromise. The exercise emphasized critical analysis of digital text manipulation and metadata-driven mapping to expose a covert campaign to reshape history.

RUSTyCurtain



how we trained

meet the mini-challenges:

In the CornerPocket challenge, students uncovered a covert data pipeline hidden across three networked machines. An image file shared by the user “EightBall” contained a concealed zip archive, which led to user credentials embedded in steganographic PDFs and images. Chained access across the machines revealed scrambled metadata pointing to a high-port FTP server masked within normal traffic. The final flag was stored in a falsified scoreboard file, requiring precise extraction and coordination. The scenario emphasized image-based steganography, credential discovery, and the dangers of hidden services in layered network environments.

CornerPocket

how we trained

meet the mini-challenges:

In the Hayloft challenge, students started by investigating inconsistencies in a farm's pig counts, where numbers were quietly manipulated in official reports. What began as a simple data-check turned deeply personal when the boy managing the farm uncovered secret messages embedded inside daily photos sent from his missing father, who had vanished during a classified space program. Through decoding hidden images and corrupted files, players realized the boy's father had been alive much longer than the family was told, sending increasingly desperate communications. As students broke into protected home devices and sifted through hidden correspondence, they pieced together a heartbreakin

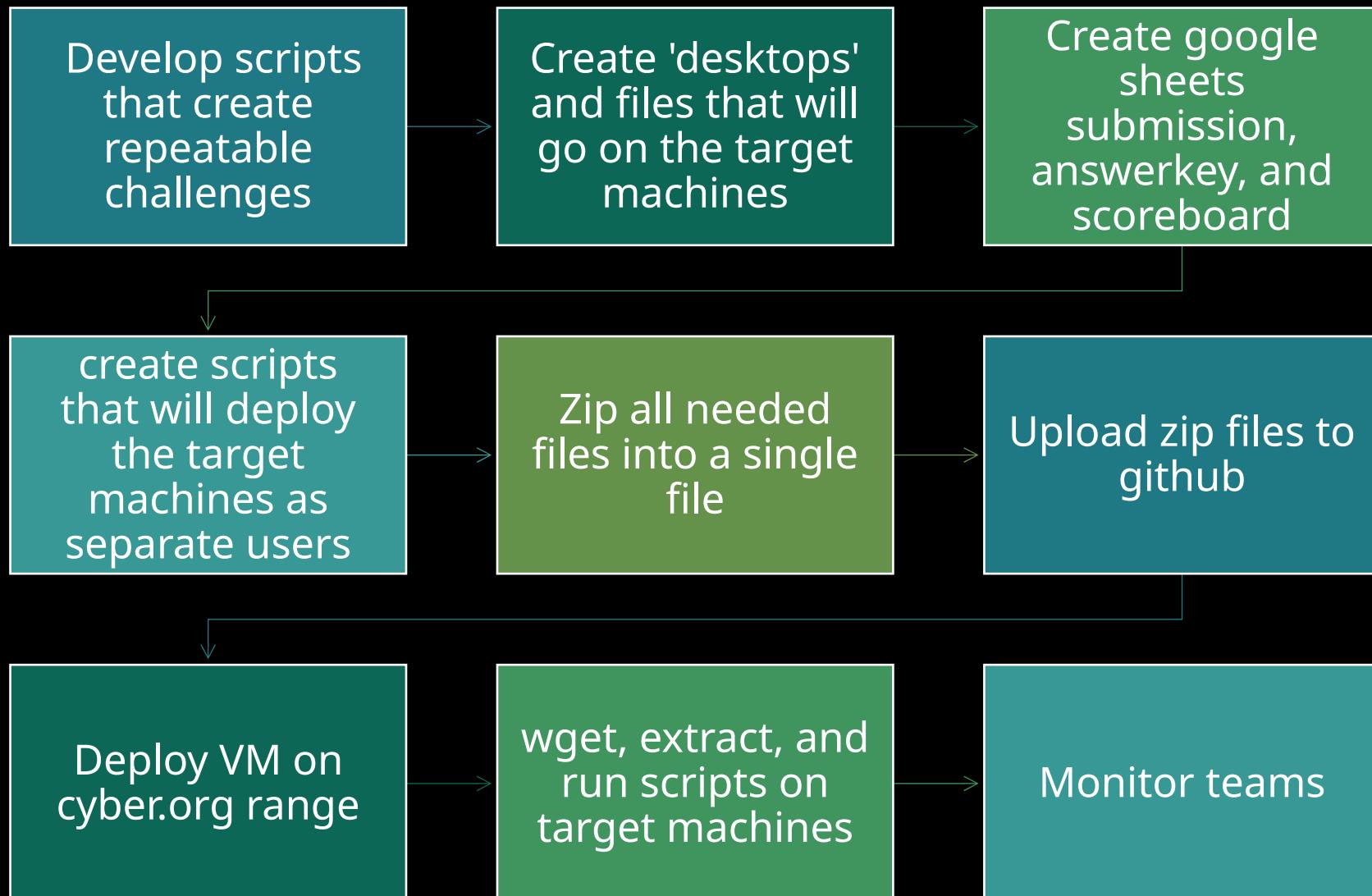
Hayloft



develop and deploy

develop and deploy

steps to
deploy a
cyber.org
challenge



develop and deploy

take explicit notes on what needs to be taught before each mini-challenge

ppsCTF / challenges / rustycurtain / **rustycurtain-prep-setup.txt** □

jboyce1 Update rustycurtain-prep-setup.txt •

Code Blame 34 lines (25 loc) · 1.38 KB ⚙️ Code 55% faster with GitHub Copilot

```
1 This is before the rusty curtain challenge to familiarize the participants with the types of things they might need
2 first, open up and access the services
3
4 Walk the students through the following from cybergate Practice and explore:
5 Step 1: Start your ubuntu machine from the cyber.org range and open up some services
6
7 start telnet
8 wget https://raw.githubusercontent.com/jboyce1/ppsCTF/main/classes/CyberCartographer/flagscripts/deploy-telnet-23.py
9 sudo python3 deploy-telnet-23.py
10
11 start an ftp server and place a file in it
12 wget https://raw.githubusercontent.com/jboyce1/ppsCTF/main/classes/CyberCartographer/flagscripts/ftp-anon-login.py
13 sudo python3 ftp-anon-login.py
14 nano test.txt
15 chmod 777 test.txt
16
17 start ssh on a highport
18 wget https://raw.githubusercontent.com/jboyce1/ppsCTF/main/classes/CyberCartographer/flagscripts/ssh-highport-generator.py
19 sudo python3 ssh-highport-generator.py
20
21 start ftp on a highport
22 wget https://raw.githubusercontent.com/jboyce1/ppsCTF/main/classes/CyberCartographer/flagscripts/ftp-anon-highport.py
23 sudo python3 ftp-anon-highport.py
24
25 Step 2: Start your kali machine from the cyber.org range try to find your open ports
26
27 MsDisin
28 Things to practice:
29 use wc to put together a phrase based on the number of words given
30 use sed and 'replaced words' to make a quote that has a famous year
31 sqlite search for most visited websites
32 sqlsearch for a spike in website usage
```

develop and deploy

write clear instructions on target deployment

```
1 note# double check ctf2.py for functionality, students were not able to see contents Feb 2025
2 instructions:
3
4 from ubuntu machine:
5 sudo git clone https://github.com/jboyce1/ppsCTF.git
6
7 Complete all the zip files on VM
8 navigate to
9 cd ppsCTF/challenges/rustycurtain
10 ls to ensure the files are there
11
12
13 run ctf1.py on as many cyber.org vms as teams are competing
14 sudo python3 ctf1.py
15 rung ctf2.py on as many cyber.org vms as teams are competing
16 sudo python3 ctf2.py
17
18 use the rustycurtainchallengemap.doc and rustycurtainanswerkey.xlsx to guide challenge.
```

how we competed

how we competed

pps{CyberTacticsFest}

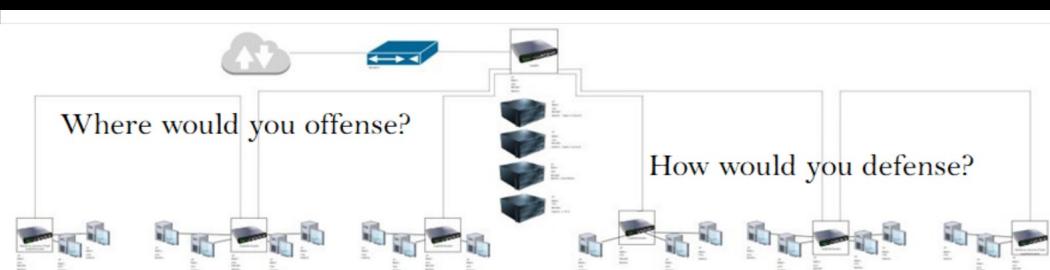
3 rounds

10 targets each round

separate environments

rules of engagement

3 'scenarios'



how we competed

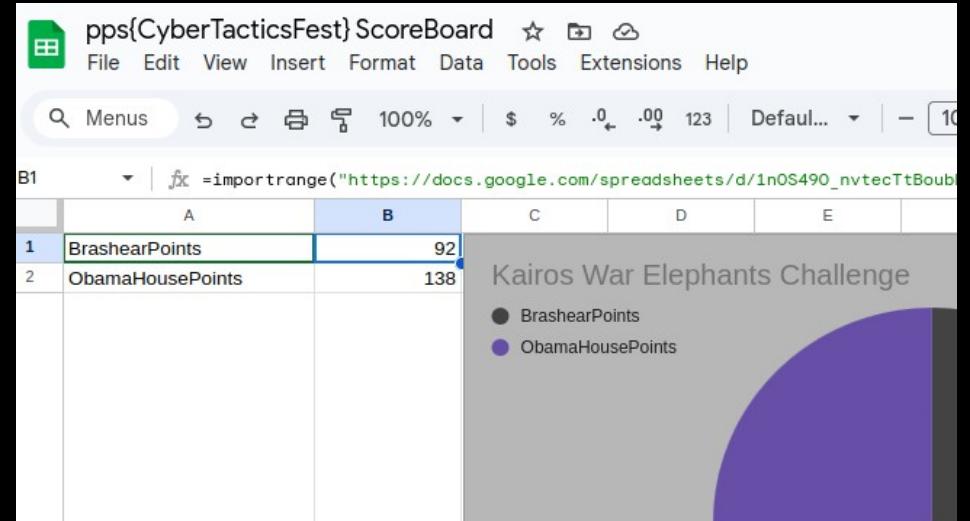
answer key

| Kairos War-Elephants Challenge AnswerKey | | |
|--|--------------------------------------|-------------------------------------|
| M5 | A | M |
| 1 | | |
| 2 | | ObamaHouseResponse |
| 3 | | ObamaHouseF |
| 4 | Flag | ObamaResponse |
| 5 | pps{1x1_Dir3ct0ryandaFil3_98hhk} | pps{1x1_F0undR00sevelt} |
| 6 | pps{1x1_NanoCat3aandir3ct0ry_987y9h} | pps{1x1_Fil3aandir3ct0ry_dfgdg} |
| 7 | pps{1x1_Fil3aandir3ct0ry_dfgdg} | pps{1x1_ThatsOneSmallStep} |
| 8 | pps{1x1_F0undR00sevelt} | pps{1x1_Fil3aandir3ct0ry_rfwer5} |
| 9 | pps{1x1_Dir3ct0ryandaFil3_9556u} | pps{1x1_Dir3ct0ryandaFil3_9556u} |
| 10 | pps{1x1_NanoCat3aandir3ct0ry_342t5} | pps{1x1_NanoCat3aandir3ct0ry_342t5} |

flag submission

| Kairos War-Dragons Challenge ObamaHouse | | |
|---|-------------------------------------|-------------|
| C1 | A | B |
| 1 | ObamaHouse | 138 |
| 2 | Flag | ObamaPoints |
| 3 | pps{1x1_F0undR00sevelt} | 1 |
| 4 | pps{1x1_Fil3aandir3ct0ry_dfgdg} | 1 |
| 5 | pps{1x1_ThatsOneSmallStep} | 1 |
| 6 | pps{1x1_Fil3aandir3ct0ry_rfwer5} | 1 |
| 7 | pps{1x1_Dir3ct0ryandaFil3_9556u} | 1 |
| 8 | pps{1x1_NanoCat3aandir3ct0ry_342t5} | 1 |
| 9 | pps{1x2_scp_krdoxz} | 2 |
| 10 | pps{1x1_MorseOverload} | 1 |

public scoreboard

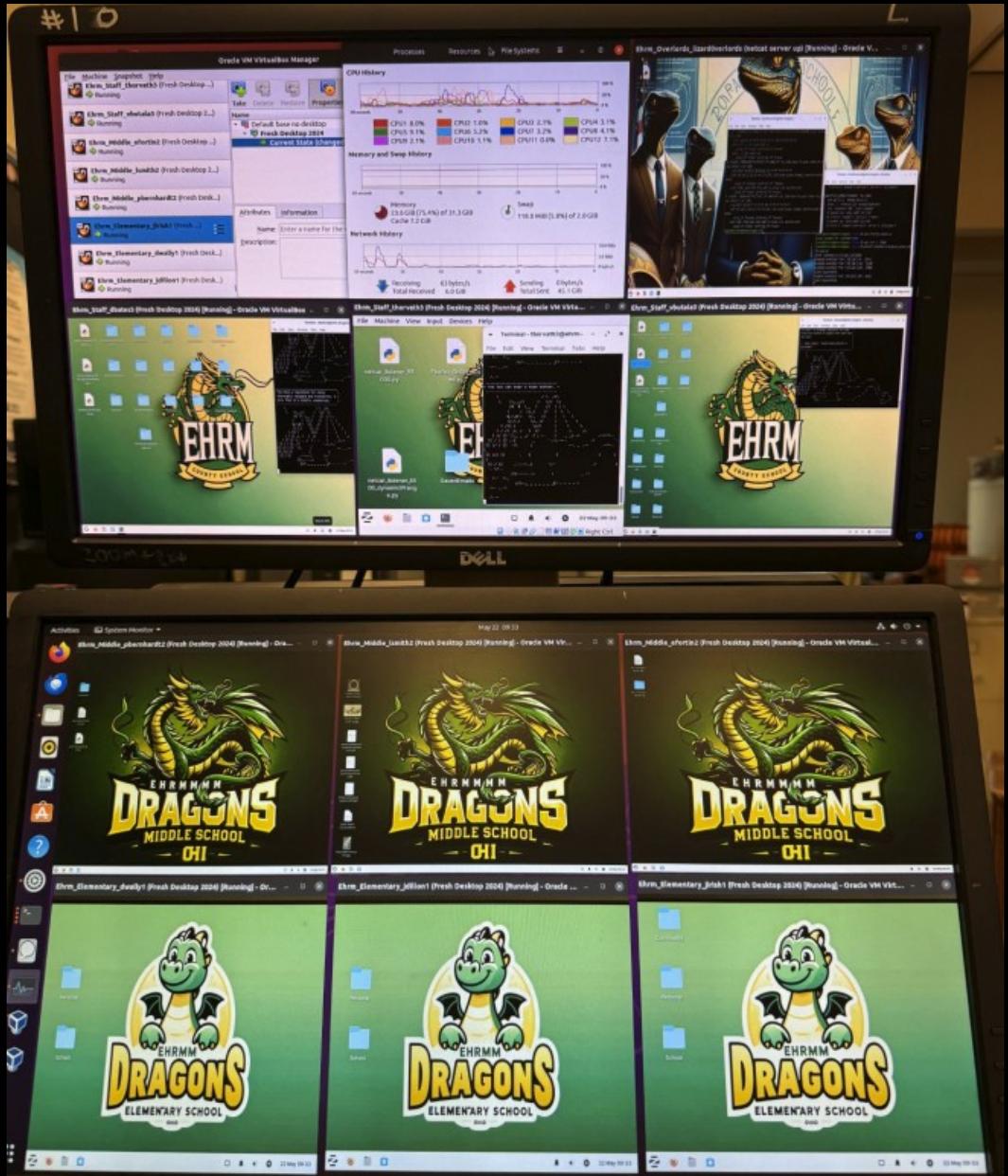


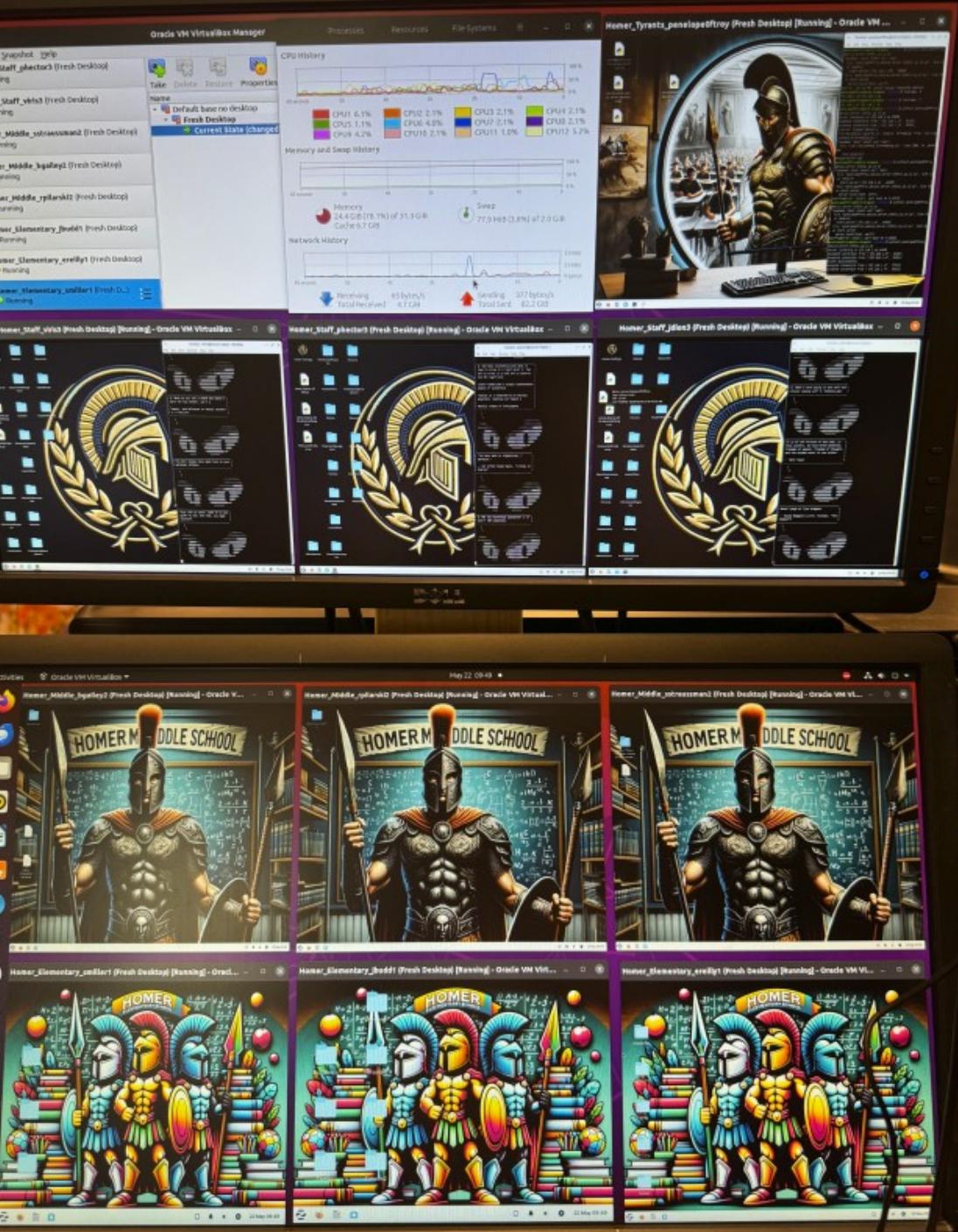
how we competed

Ehrm, Dragons

scenario overview:

lizard people overlords
are biology teachers
with an agenda teach
students lizards are
superior beings





how we competed
Homers, Trojans
scenario overview:
track coaches are immortal
greek warriors sent to
find Odysseus but got
lost in the search and
are now keeping greek
warfare alive



how we competed

Kairos, War Elephants

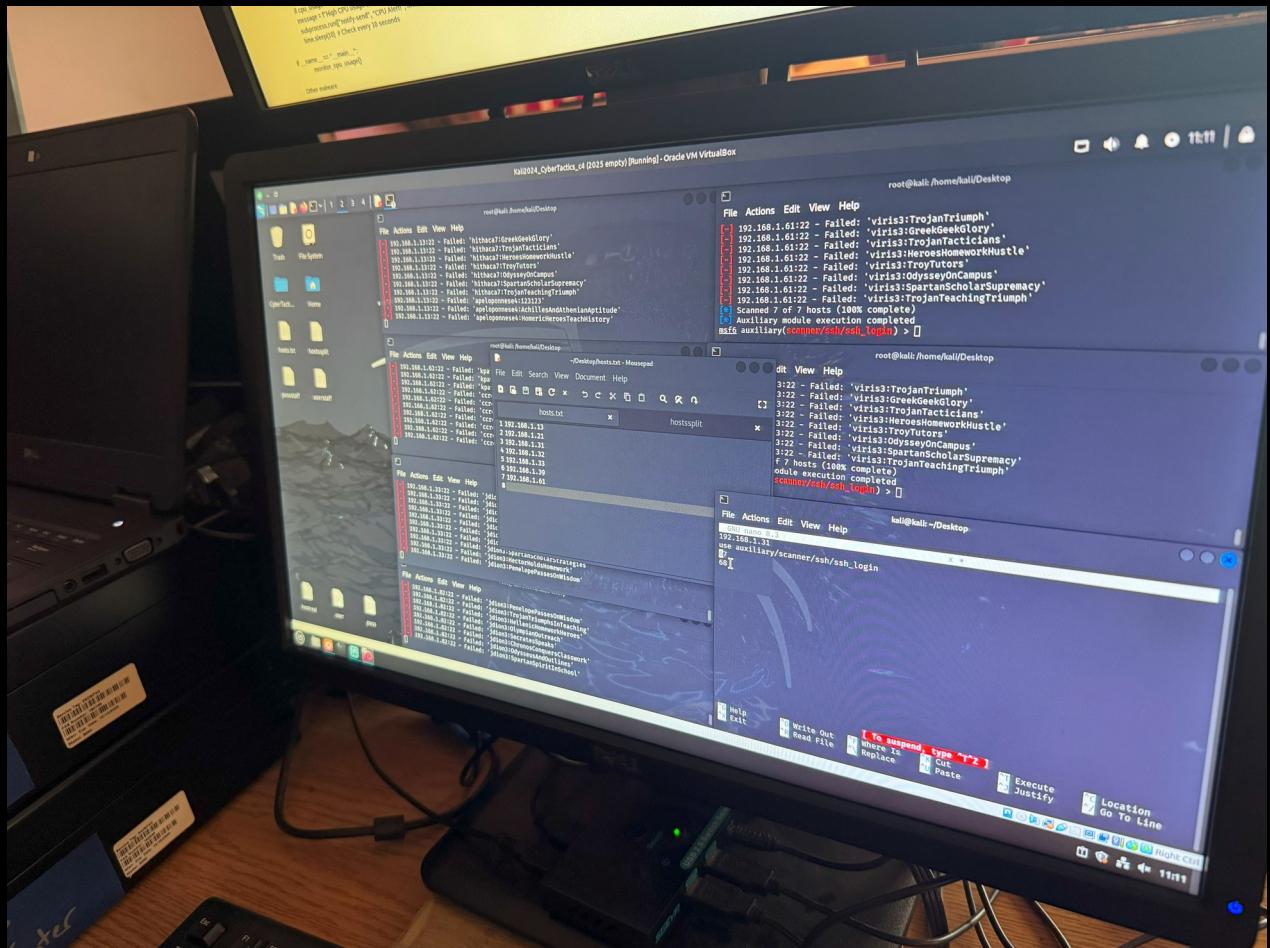
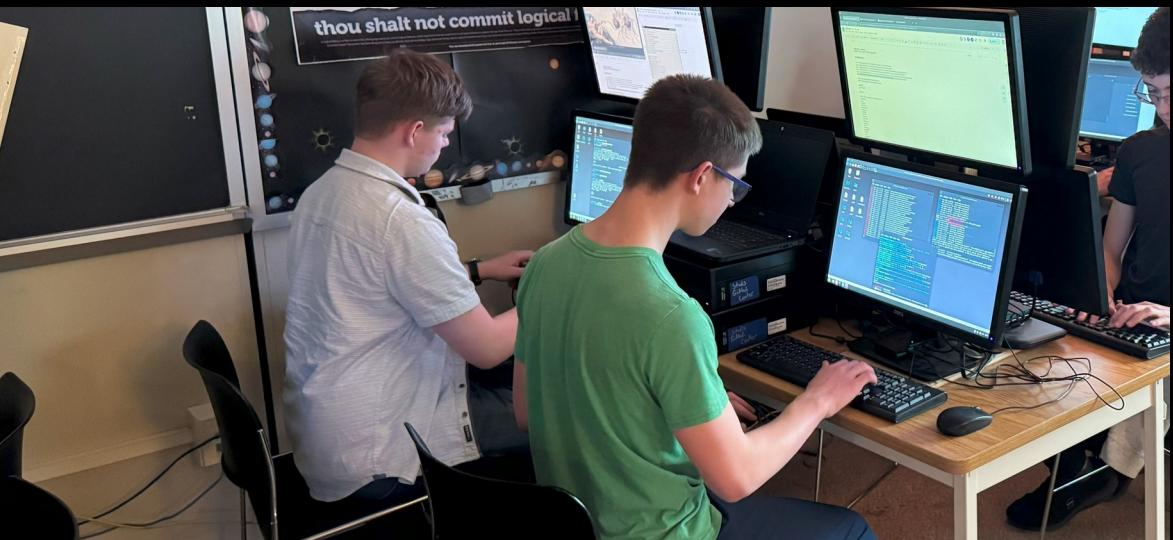
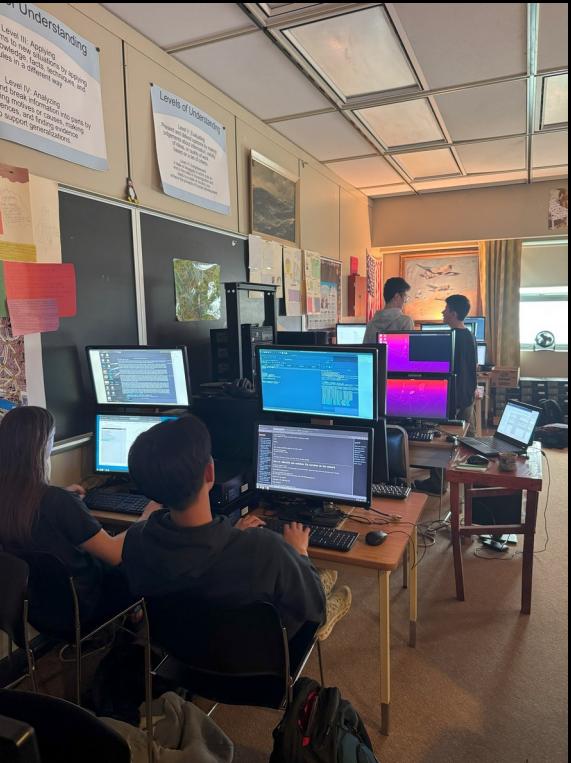
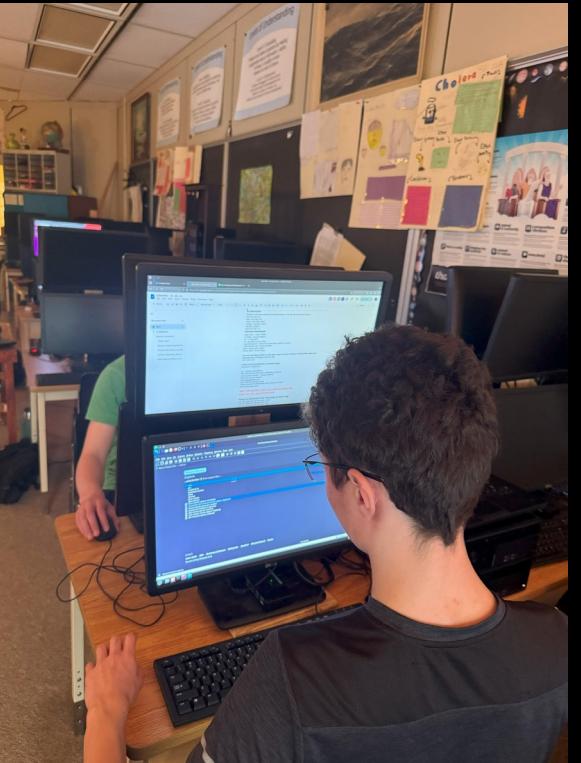


scenario overview:

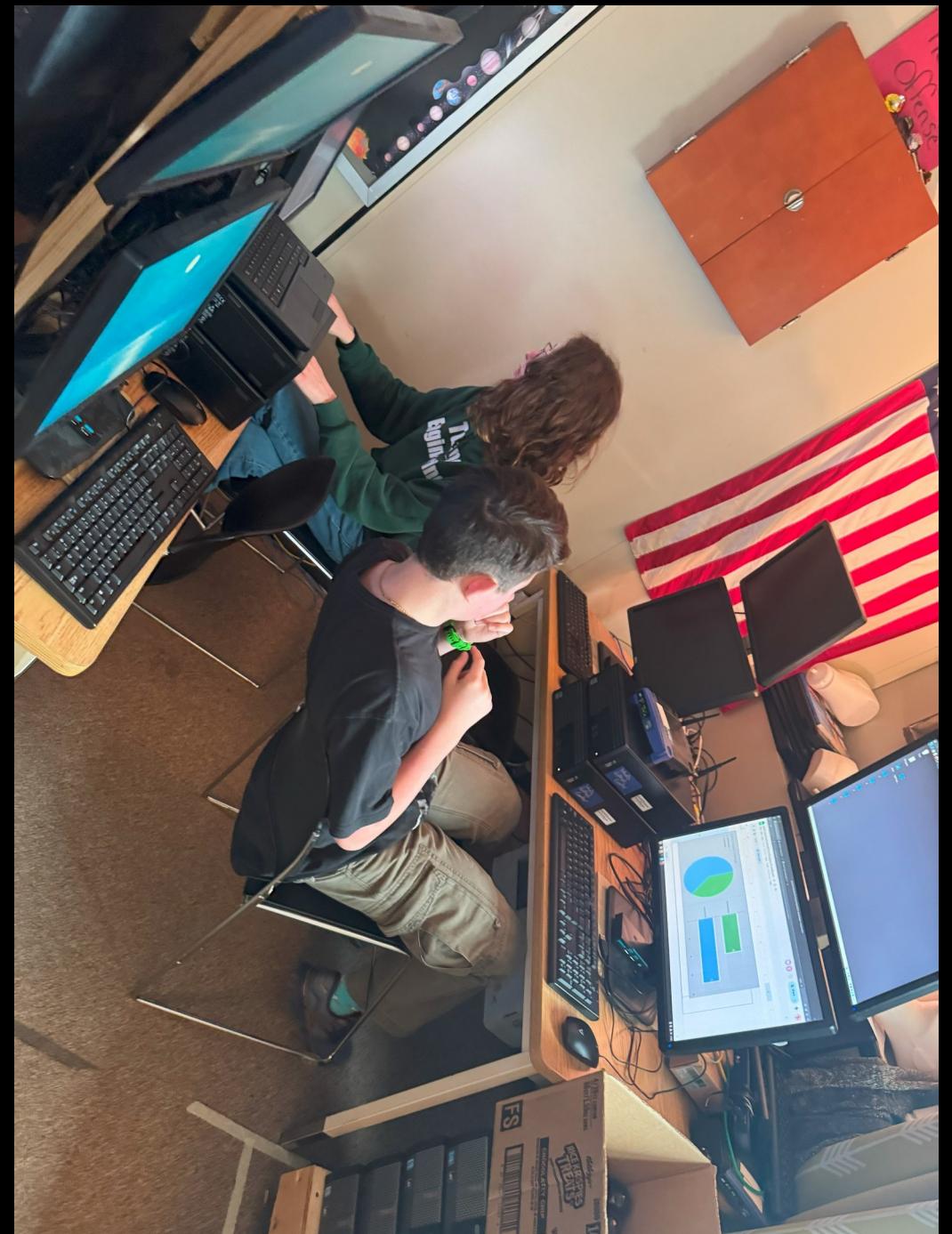
a history teacher brings back real historical figures through a time portal that are trying to flush brain rot from modern youth



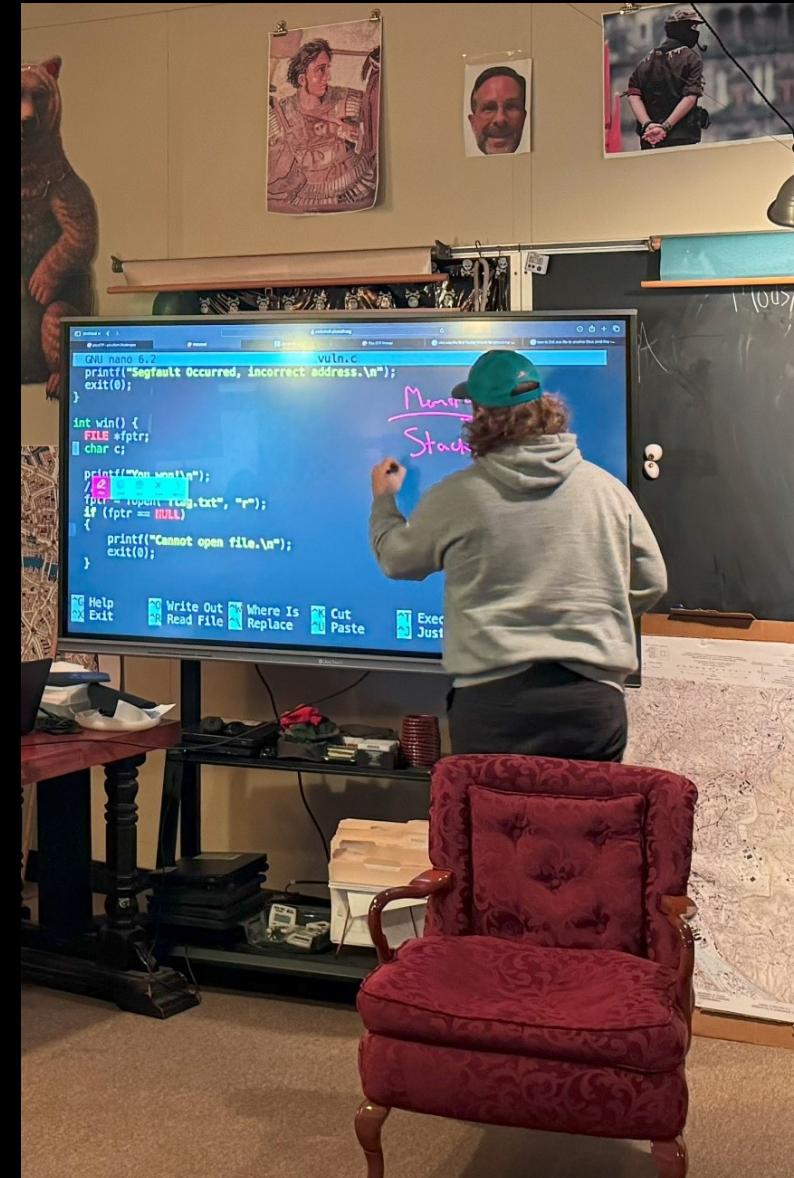
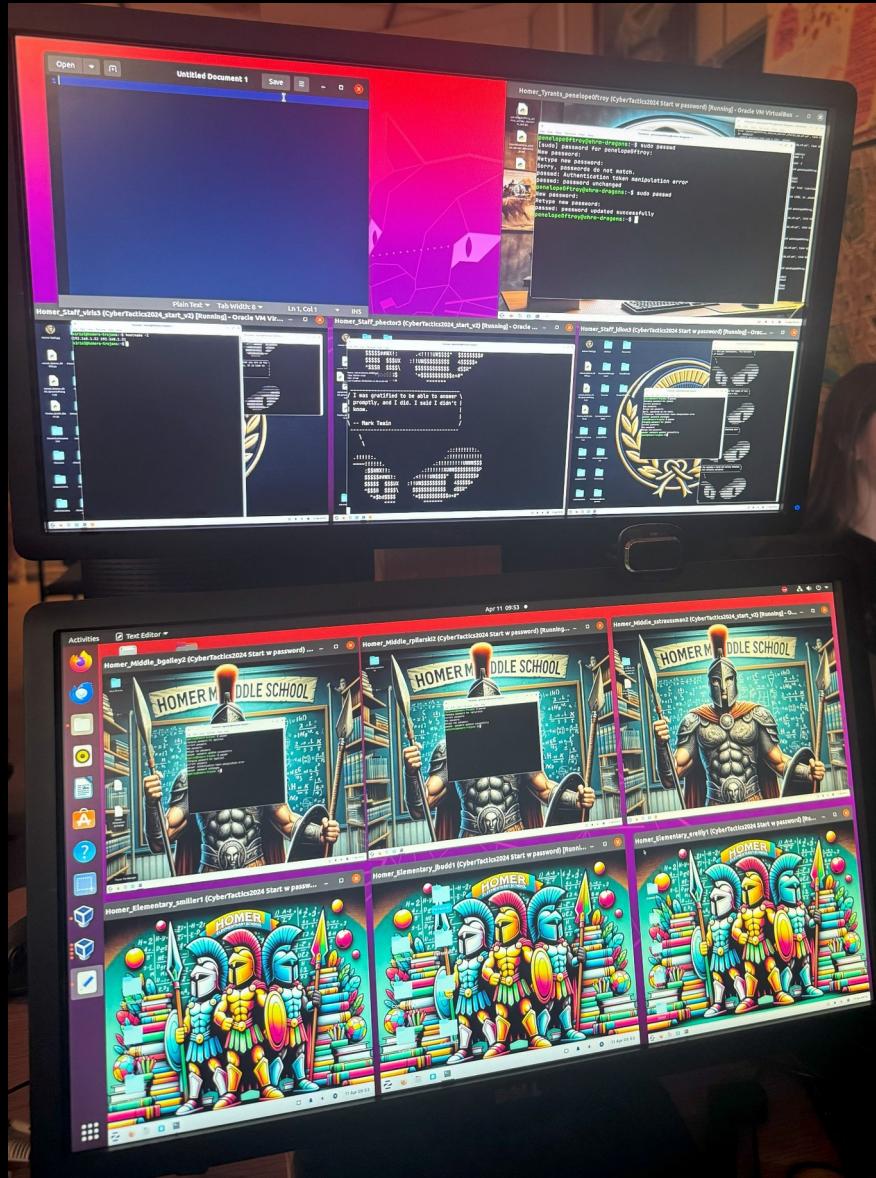
how we competed



how we competed



how we competed



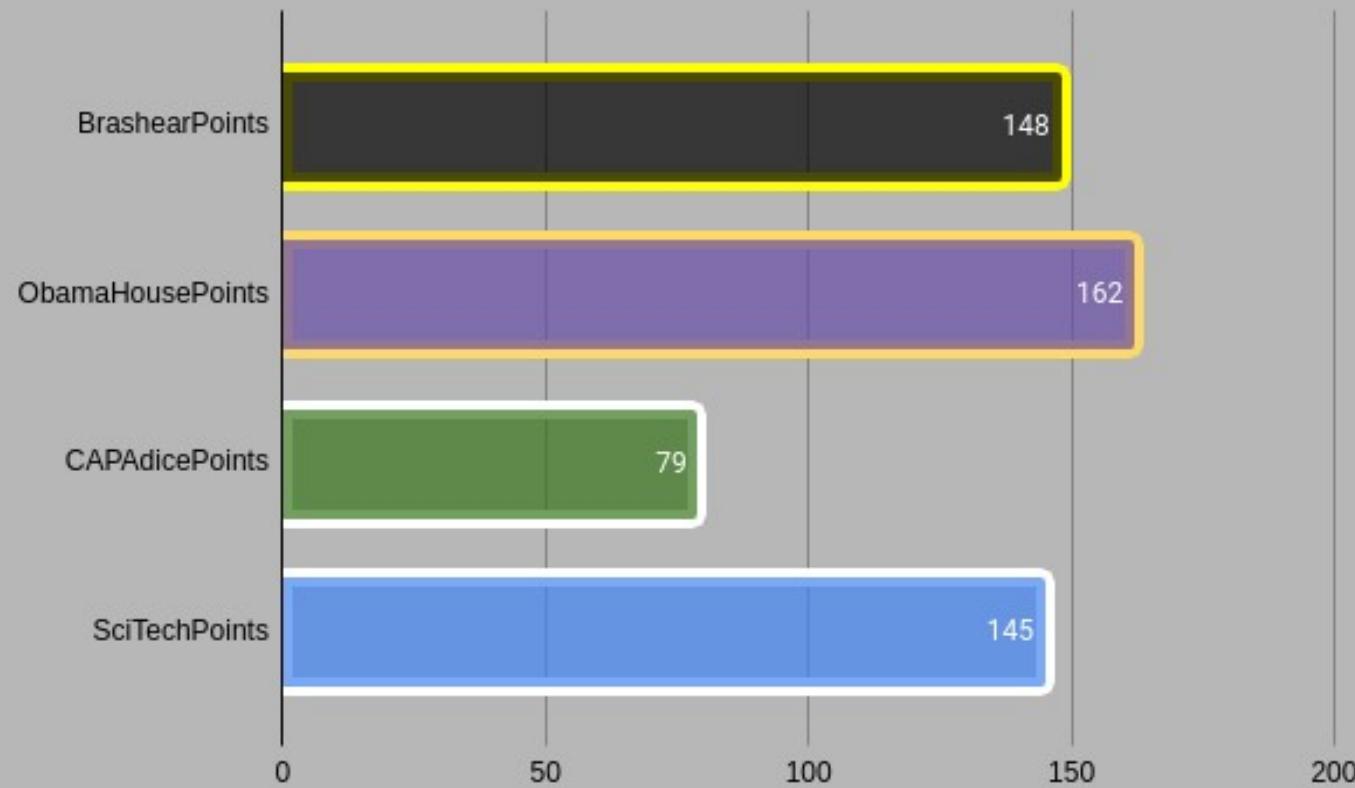
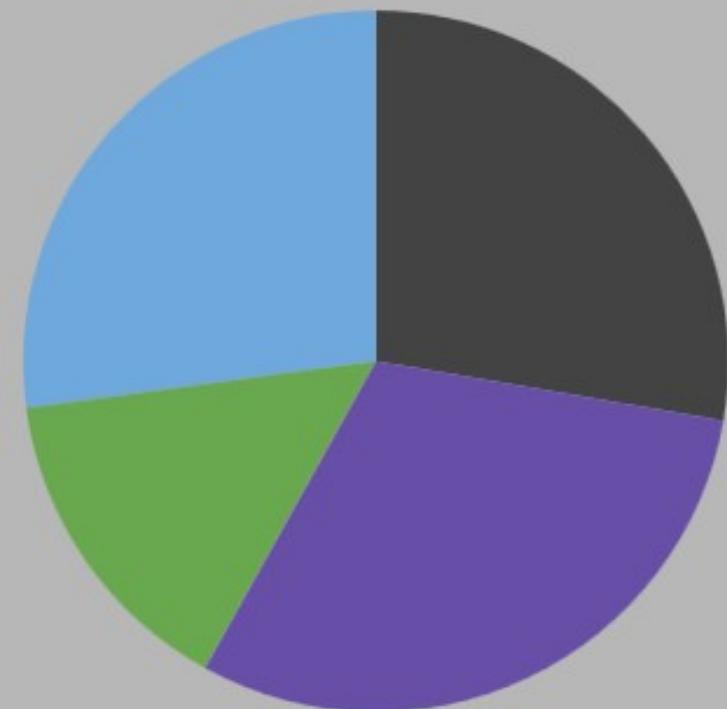
competition results

competition results

Round 1

Ehrm Dragons Challenge

- BrashearPoints
- ObamaHousePoints
- CAPAdicePoints
- SciTechPoints

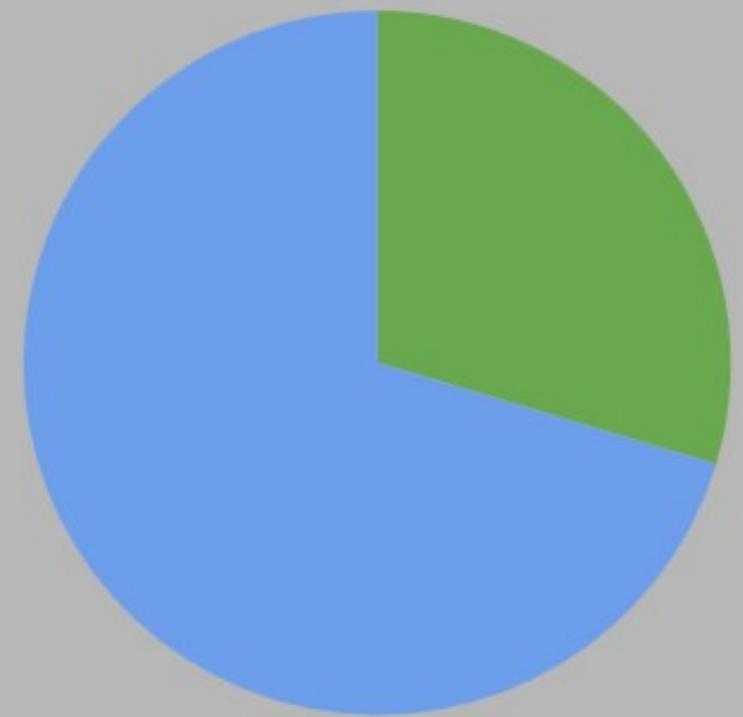


competition results

Round 2 (losers vs losers)

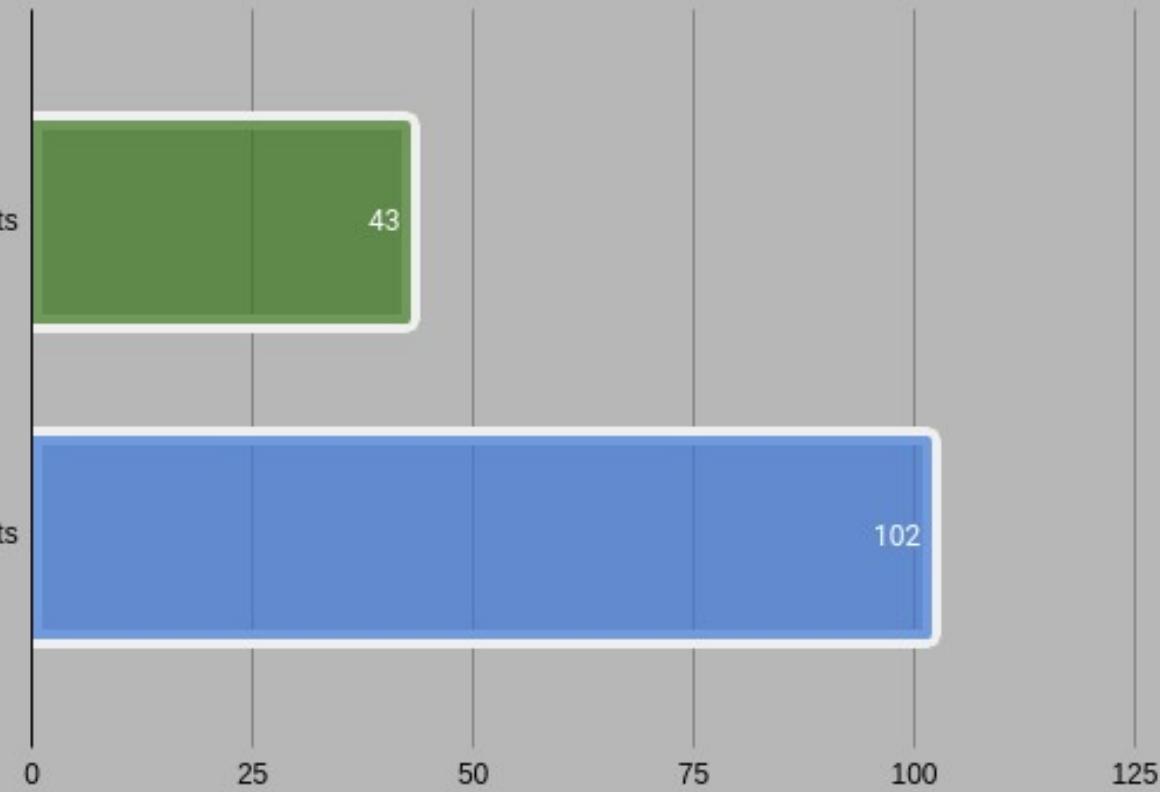
Homer Dragons Challenge

- CAPAdicePoints
- SciTechPoints



CAPAdicePoints

SciTechPoints

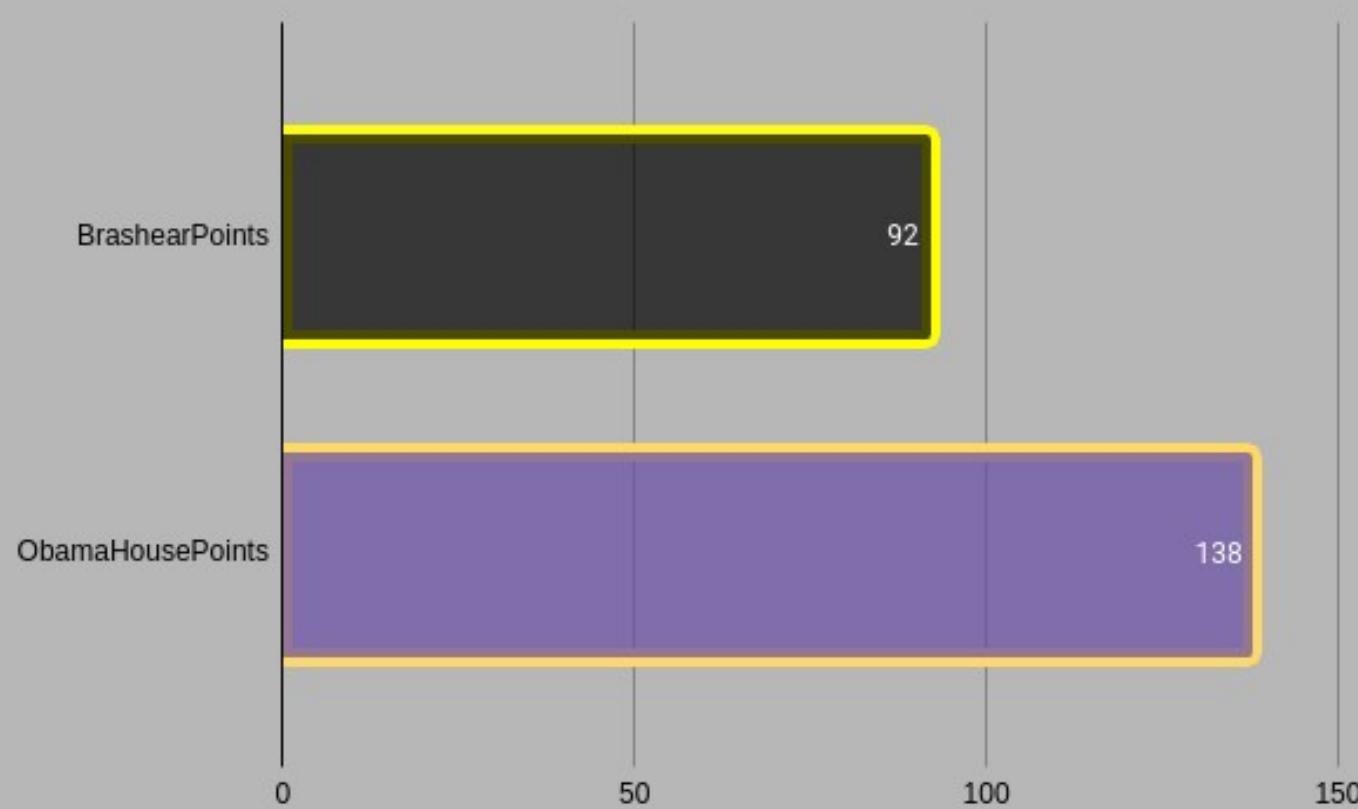
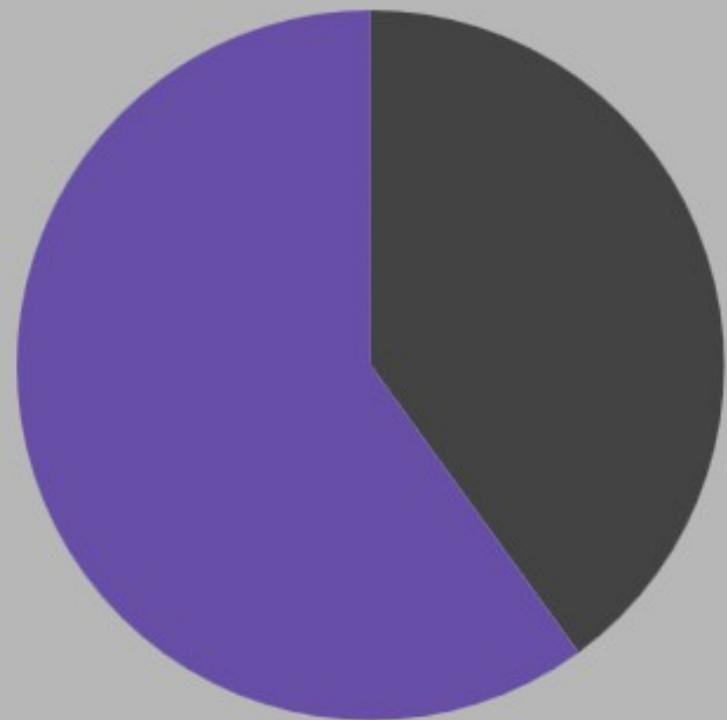


competition results

Round 3 (winners vs winners)

Kairos War Elephants Challenge

- BrashearPoints
- ObamaHousePoints



outcomes

outcomes

-  students on SciTech developed shared documentation and worked as a well oiled machine
-  students from Brashear hot swapped seats to complete challenges based on strengths
-  students from ObamaHouse made the development of challenges for next season into a long-term class project
-  students from CAPdice used untaught resources (hashcat) and wrote python scripts to solve challenges

next steps

-  develop non-profit (CyberTacticsForge) to facilitate voucher scholarships, intern opportunities, infrastructure upgrades
-  identify additional mentors; clarify work-roles and expectations
-  involve more schools from SW PA and OH
-  develop capability to deploy more persistent target boxes for more complex
-  focus on defensive actions; seconion and firewalls

express an interest

questions/
remarks



Share your feedback!

In your Accelevents app, click "View Details" for this session, then "Survey" on the Activity tab to complete a quick survey and let us know what you thought of this session.

