



2025 CAE Community Symposium

Experiential Learning Competencies: How Hackathons Intersect Cybersecurity Education Competencies Using Industry Partnerships

Christian Servin, J.J. Childress, and Nadia Karichev

El Paso Community College, El Paso TX, USA

Introduction/ Background



- **Hackathons as Experiential Learning**

- Utilized in cybersecurity education through capture-the-flag (CTF) competitions and challenge-based activities.
- Serve as platforms to bridge educational requirements with industry needs.

- **Institutional Constraints**

- Limited course contact hours.
- Insufficient resources for organizing and supporting events.
- Challenges in faculty mentoring and project development.
- Impact on students' ability to meet industry and workforce requirements.

- **Cybersecurity Workforce Alignment**

- CAE-CD mandates integration of competencies aligned with NICE and DCWF frameworks.
- Frameworks outline tasks, knowledge, and skills but often lack practical program alignment.

About Project



- **Experiential Learning as a Solution**

- Hackathons, CTF competitions, and national challenges address competency gaps.
- These activities provide hands-on experience but face logistical and institutional barriers.

- **Proposed Hackathon Framework**

- Based on the Essential Elements (ABCDE) model (Nestler & Fowler, 2023).
- Implemented in a community college setting.
- Three-day format fostering collaboration between academia and industry.

- **Industry Collaboration & Coaching**

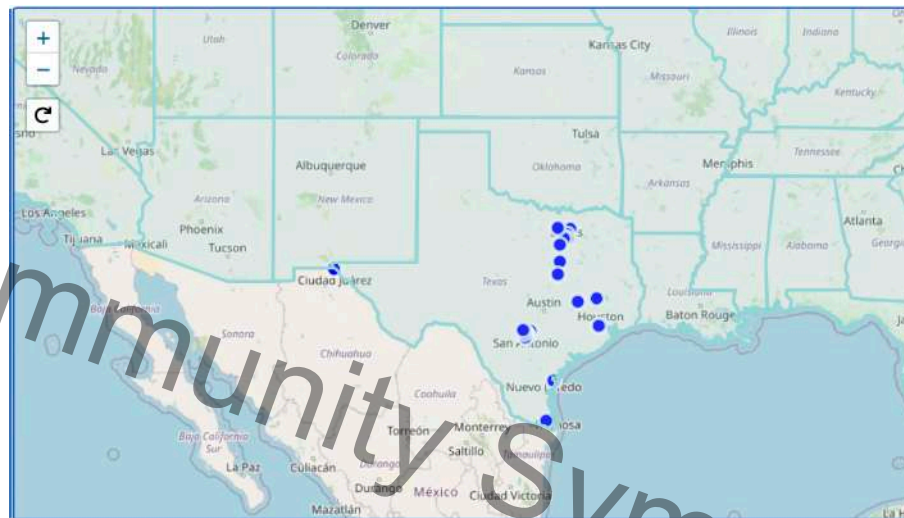
- Active participation from industry professionals.
- Work-based learning opportunities, including mentoring, cooperative work experiences, and service learning.

- **Integration of Adversarial Thinking**

- Enhances the educational impact of hackathons.
- Addresses dynamic cybersecurity education needs.



- **Borderplex Region:** Serves 2.5M people, the largest bilingual & binational workforce.
- **HSI:** 85%+ Hispanic students (EPCC 2020).
- **Location:** Near Fort Bliss, White Sands, 500 miles from Dallas & Houston.
- **Education:** 18 Dual Credit, 18 ECHS, 19 P-TECH programs.
- **STEM:** 2+2 MOU, including Computer Science.
- **Cybersecurity:** NCAE-CD (2024–2029), DHS & NSA recognized.
- **Strategy:** Cyber Strategy (2018), adversarial thinking curriculum.
- **NSF Grant:** NSF DUE-2300378, expanding cybersecurity through Adversarial Thinking in El Paso, Cd. Juarez, & Las Cruces.

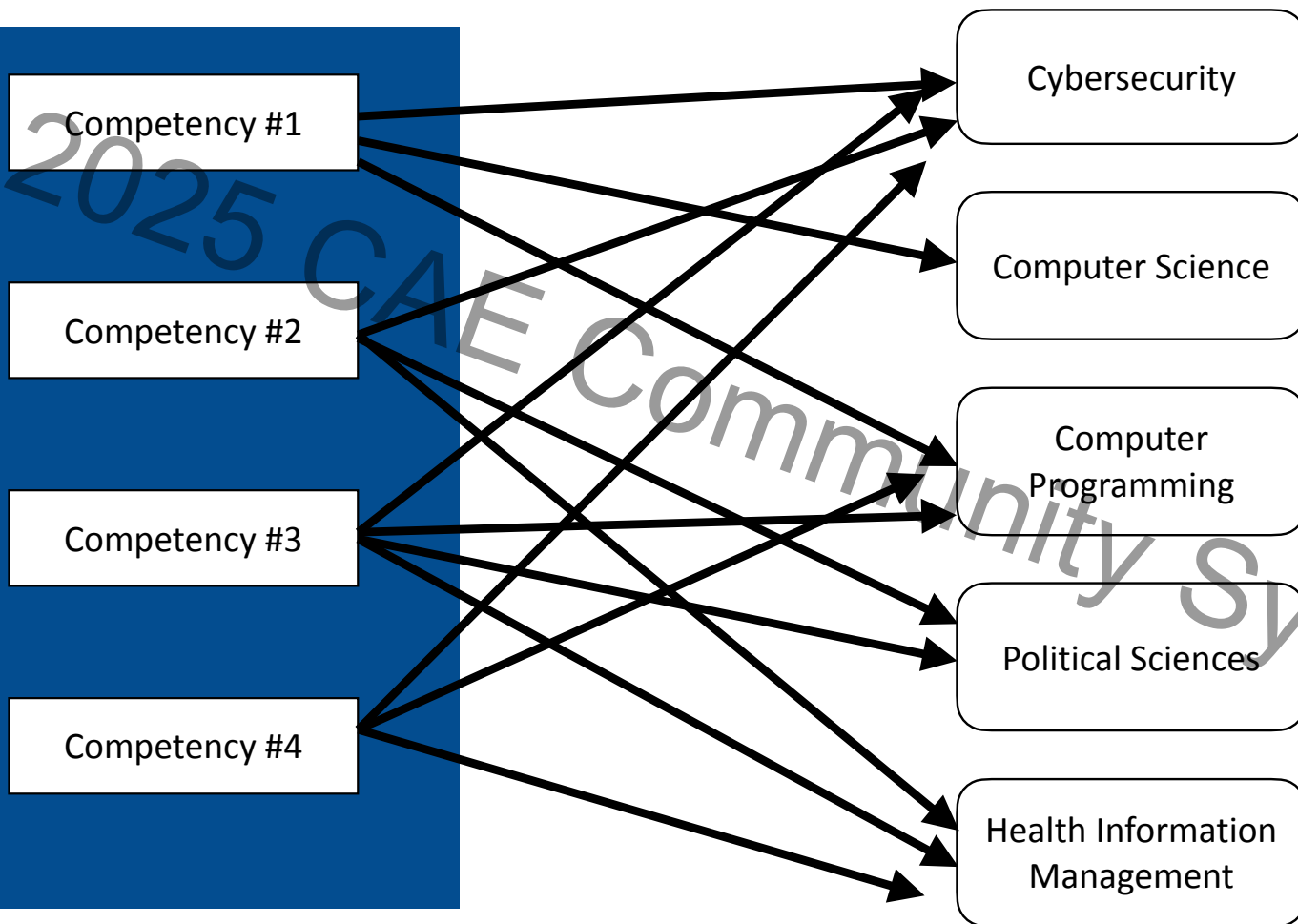


26 Institutions in Texas



CAE
IN CYBERSECURITY
COMMUNITY







Competency #1

Competency #2

Competency #3

Competency #4

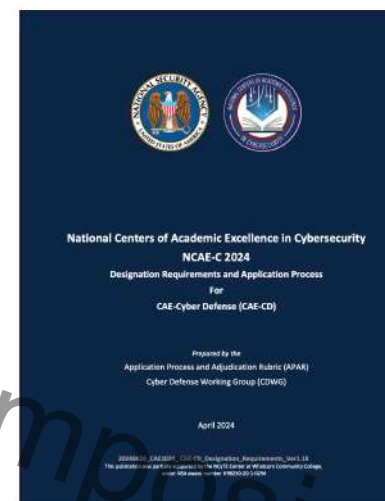
Cybersecurity

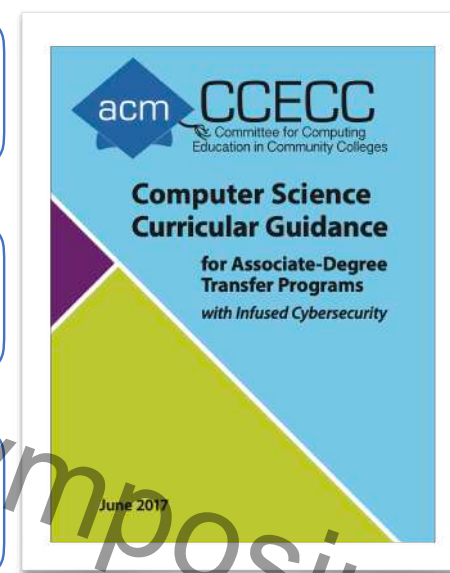
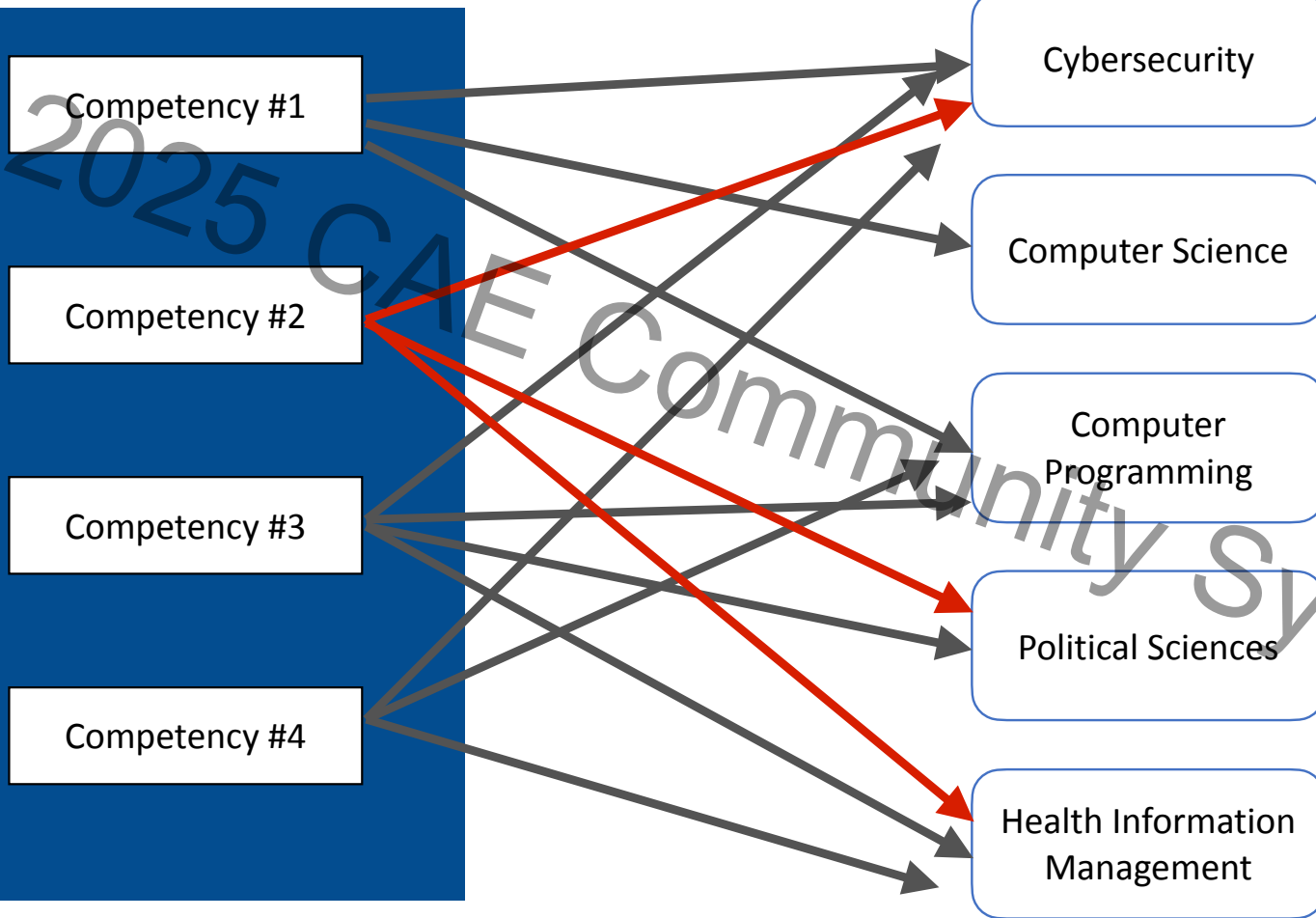
Computer Science

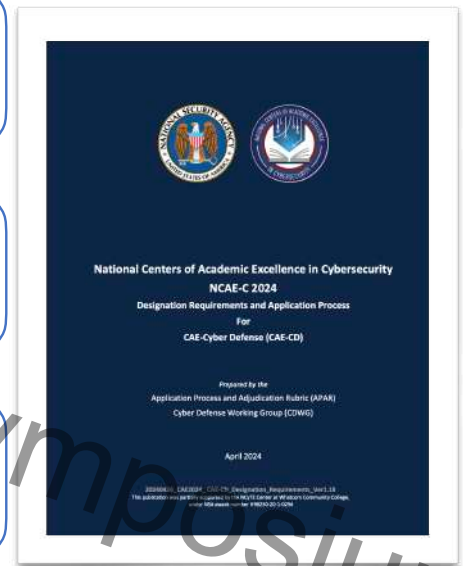
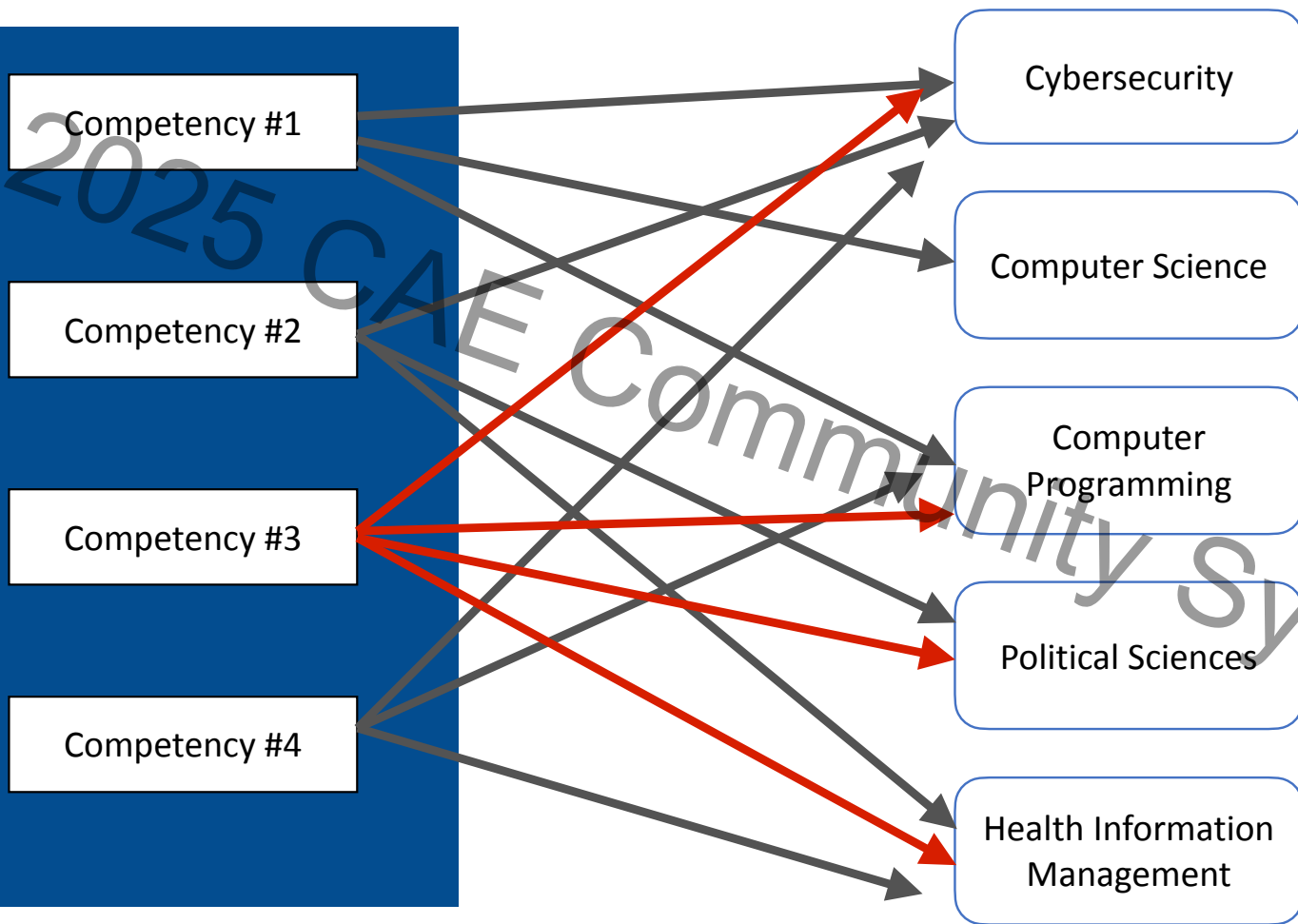
Computer Programming

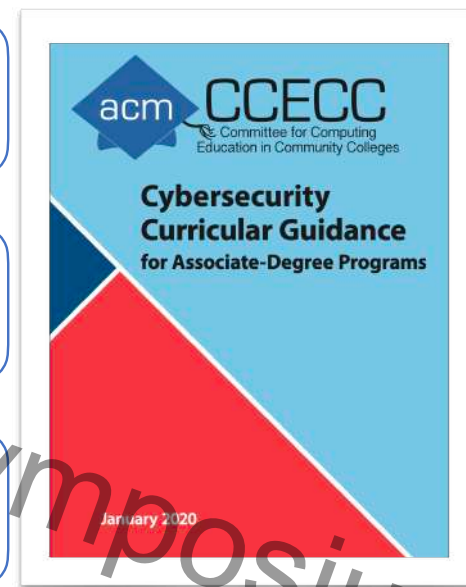
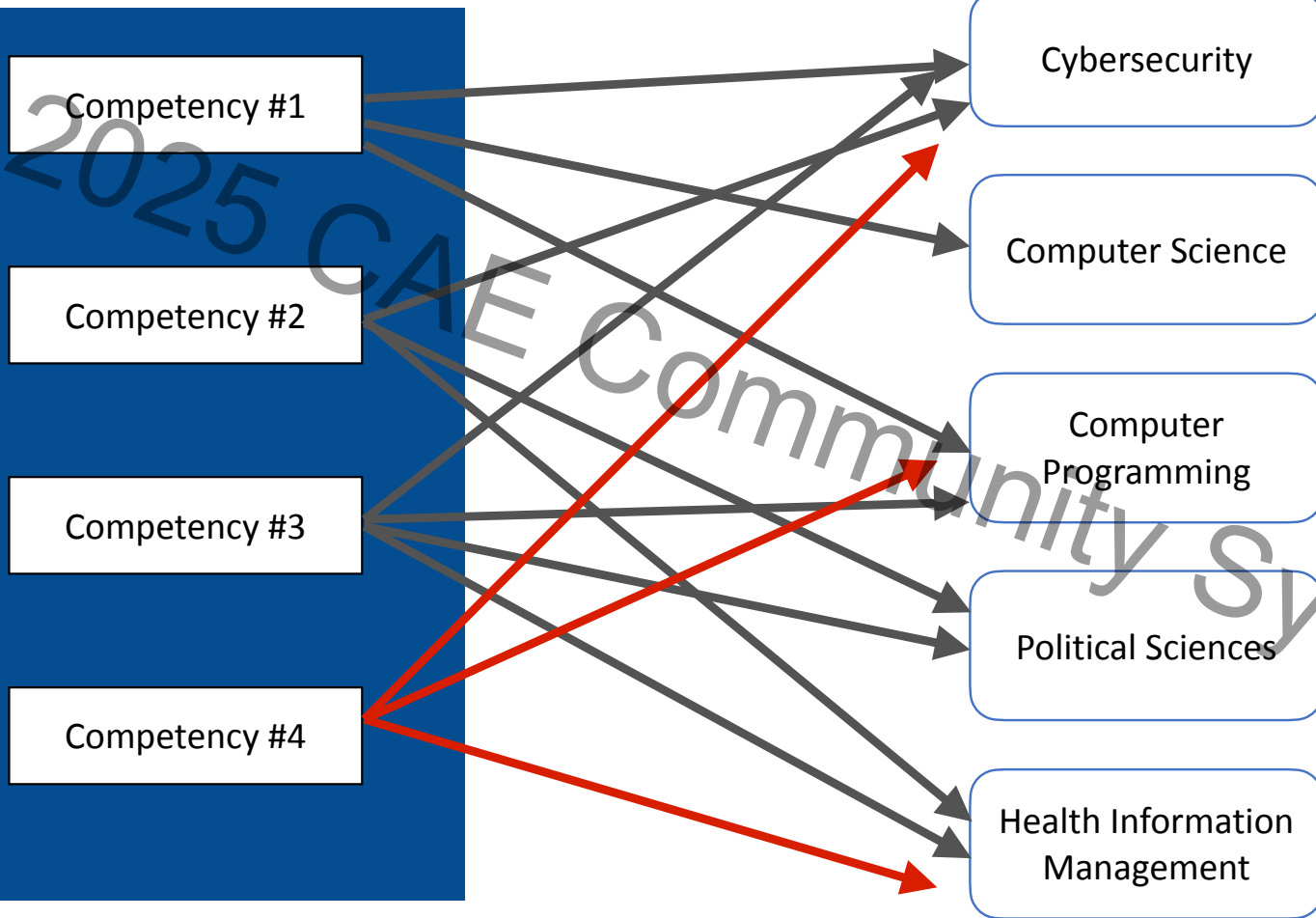
Political Sciences

Health Information Management









Competency #1

Competency #2

Competency #3

Competency #4

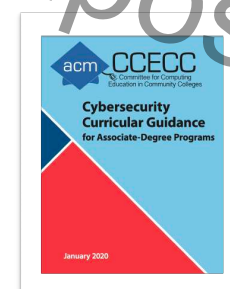
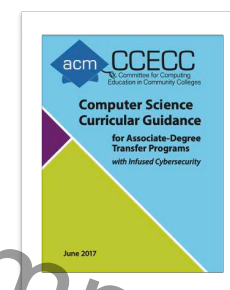
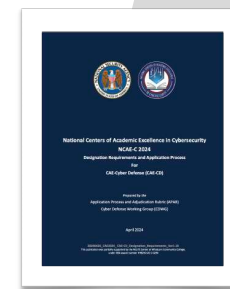
Cybersecurity

Computer Science

Computer Programming

Political Sciences

Health Information Management



CAE
IN CYBERSECURITY
COMMUNITY



CAE
IN CYBERSECURITY
COMMUNITY

DEFINITION AND 5 ESSENTIAL ELEMENTS

"Competency is the ability of the individual to complete a task in the context of a work role."

ACTOR	BEHAVIOR	CONTEXT	DEGREE	EMPLOYABILITY
Who	What	How	How much	Professional Skills
Description of student, and required knowledge and skills	References a task from the DCWF or NICE framework.	Describes how this task is enacted through a classroom or extra-curricular activity	Defines parameters of competency in terms of time, accuracy, and/or completion.	Identifies the professional (soft) skills necessary to do this task in a work role.

Work-roles in El Paso TX



Work-role: Cyber Defense Forensics Analyst. Competency Statement: As a graduate with an AAS in Cybersecurity, demonstrate the ability to use data from various cyber defense tools to analyze events and mitigate threats. This role includes leveraging scripts to operationalize data, supporting SCADA system components in contested environments, and analyzing threat information from multiple sources. Additionally, analyze digital evidence and investigate computer security incidents to derive useful information for system and network vulnerability mitigation.

Work-role: All-Source Analyst. Competency Statement: As a graduate with an AAS in Cybersecurity, demonstrate the ability to use data from various cyber defense tools to analyze events and mitigate threats. This role includes supporting SCADA system components in contested environments and analyzing threat information from multiple sources to draw insights and understand implications.

Work-role: Cyber Defense Analyst. Competency Statement: As a graduate with an AAS in Cybersecurity from a two-year college, demonstrate the ability to use data collected from various cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events within their environment to mitigate threats. This role includes analyzing and reporting system and organizational security posture trends, and isolating and removing malware in a contested environment.

Work-role: Cyber Defense Infrastructure Support. Competency Statement: As a graduate with an AAS in Cybersecurity, demonstrate the ability to assess and respond to risks, cyber defense threats, and security design principles affecting information systems. This includes testing, implementing, deploying, maintaining, reviewing, and administering infrastructure hardware and software for network defense. Additionally, possess the skills to monitor networks and actively remediate unauthorized activities to ensure continuous protection of information systems.

Category		Details
Name of Competency		Capture-the-Flag (CTF) Cybersecurity and Digital Forensics
Type of Activity		Capture the Flag (CTF)
Associated work role as listed in DCWF or NICE		Digital Forensics
Actor	Type of Student	An El Paso Community College student with foundational knowledge of Linux, cryptography, and forensic analysis participating in a Capture the Flag (CTF) competition
	Necessary knowledge and/or skills	
Behavior	Task The student will demonstrate cybersecurity and digital forensics skills by executing the following tasks	T1548: Determine adequacy of access controls T0167: Perform file signature analysis T0179: Perform static media analysis T1121: Decrypt seized data T1191: Determine relevance of recovered data T1322: Capture network traffic associated with malicious activities T1323: Analyze network traffic associated with malicious activities T1607: Recover information from forensic data sources
Context	Scenario	Students working teams on provided Linux machines to solve CTF challenges focused on Linux system navigation, hashing, cryptography, steganography, and basic forensic analysis. Challenges involve real-world scenarios such as decoding hidden messages, recovering deleted files, and cracking password hashes. Tools used include Linux terminal commands (e.g., find, grep, awk, strings, cat, tar), cryptographic utilities (openssl, gpg), forensic tools (binwalk, foremost, steghide), packets capture (e.g., Wireshark), and hash cracking tools (john, hashcat). Students document their approach, tools used, and methodology for solving challenges.
	Technology	
	Documentation	
	Limitations	
Degree	% Complete (if stated)	Successfully solve CTF challenges in different categories (Linux navigation, hashing, cryptography, steganography, forensics) and submit a detailed report documenting the techniques used, commands executed, and solutions achieved, 4 hours
	% Correct (if stated)	
	Amount of Time (if stated)	
Employability	(use Montreat 360)	Teamwork. Contribute to a Common Goal: Ability to take individual responsibility for assigned tasks and working together to achieve a common purpose. Critical Thinking, Think Creatively: Identify or derive alternative interpretations of data or observations, recognize new information that might support or contradict a hypothesis, explain how new information can change their understanding and ability to address a problem. Learn and Problem Solve: Ability to separate relevant and irrelevant information, integrate multiple sources of information to solve problems, and learn and apply new information to solve real-world issues.



Category	Details
Name of Competency	Capture-the-Flag (CTF) Cybersecurity and Digital Forensics
Type of Activity	Capture the Flag (CTF)
Associated work role as listed in DCWF or NICE	Digital Forensics

Actor	Type of Student	An El Paso Community College student with foundational knowledge of Linux, cryptography, and forensic analysis participating in a Capture the Flag (CTF) competition	
	Necessary knowledge and/or skills		
Behavior	Task	T1548: Determine adequacy of access controls T0167: Perform file signature analysis T0179: Perform static media analysis T1121: Decrypt seized data T1191: Determine relevance of recovered data T1322: Capture network traffic associated with malicious activities T1323: Analyze network traffic associated with malicious activities T1607: Recover information from forensic data sources	
	The student will demonstrate cybersecurity and digital forensics skills by executing the following tasks		
	Documentation	(binwalk, foremost, steghide), packets capture (e.g., Wireshark), and hash cracking tools (john, hashcat). Students document their approach, tools used, and methodology for solving challenges.	
		Limitations	
	Degree	% Complete (if stated)	Successfully solve CTF challenges in different categories (Linux navigation, hashing, cryptography, steganography, forensics) and submit a detailed report documenting the techniques used, commands executed, and solutions achieved, 4 hours
		% Correct (if stated)	
		Amount of Time (if stated)	
	Employability	(use Montreat 360)	Teamwork. Contribute to a Common Goal: Ability to take individual responsibility for assigned tasks and working together to achieve a common purpose. Critical Thinking, Think Creatively: Identify or derive alternative interpretations of data or observations, recognize new information that might support or contradict a hypothesis, explain how new information can change their understanding and ability to address a problem. Learn and Problem Solve: Ability to separate relevant and irrelevant information, integrate multiple sources of information to solve problems, and learn and apply new information to solve real-world issues.



Category		Details
Name of Competency		Capture-the-Flag (CTF) Cybersecurity and Digital Forensics
Type of Activity		Capture the Flag (CTF)
Associated work role as listed in DCWF or NICE		Digital Forensics
Actor	Type of Student	An El Paso Community College student with foundational knowledge of Linux, cryptography, and forensic analysis participating in a Capture the Flag (CTF) competition
	Necessary knowledge and/or skills	
Behavior	Task	T1548: Determine adequacy of access controls T0167: Perform file signature analysis T0179: Perform static media analysis T1121: Decrypt seized data T1191: Determine relevance of recovered data T1322: Capture network traffic associated with malicious activities T1323: Analyze network traffic associated with malicious activities

Context	Scenario	Students working teams on provided Linux machines to solve CTF challenges focused on Linux system navigation, hashing, cryptography, steganography, and basic forensic analysis. Challenges involve real-world scenarios such as decoding hidden messages, recovering deleted files, and cracking password hashes. Tools used include Linux terminal commands (e.g., find, grep, awk, strings, cat, tar), cryptographic utilities (openssl, gpg), forensic tools (binwalk, foremost, steghide), packets capture (e.g., Wireshark), and hash cracking tools (john, hashcat). Students document their approach, tools used, and methodology for solving challenges.
	Technology	
	Documentation	
	Limitations	

Employability	(use Montreat 360)	<p>Teamwork: Contribute to a Common Goal: Ability to take individual responsibility for assigned tasks and working together to achieve a common purpose.</p> <p>Critical Thinking, Think Creatively: Identify or derive alternative interpretations of data or observations, recognize new information that might support or contradict a hypothesis, explain how new information can change their understanding and ability to address a problem. Learn and Problem Solve: Ability to separate relevant and irrelevant information, integrate multiple sources of information to solve problems, and learn and apply new information to solve real-world issues.</p>
---------------	--------------------	---

Category		Details
Name of Competency		Capture-the-Flag (CTF) Cybersecurity and Digital Forensics
Type of Activity		Capture the Flag (CTF)
Associated work role as listed in DCWF or NICE		Digital Forensics
Actor	Type of Student	An El Paso Community College student with foundational knowledge of Linux, cryptography, and forensic analysis participating in a Capture the Flag (CTF) competition
	Necessary knowledge and/or skills	
Behavior	Task The student will demonstrate cybersecurity and digital forensics skills by executing the following tasks	T1548: Determine adequacy of access controls T0167: Perform file signature analysis T0179: Perform static media analysis T1121: Decrypt seized data T1191: Determine relevance of recovered data T1322: Capture network traffic associated with malicious activities T1323: Analyze network traffic associated with malicious activities T1607: Recover information from forensic data sources
Context	Scenario	Students working teams on provided Linux machines to solve CTF challenges focused on Linux system navigation, hashing, cryptography, steganography, and basic forensic analysis. Challenges involve real-world scenarios such as decoding hidden messages, recovering deleted files, and cracking password hashes. Tools used include Linux terminal commands (e.g., find, grep, awk, strings, cat, tar), cryptographic utilities (openssl, gpg), forensic tools (binwalk, foremost, steghide), packets capture (e.g., Wireshark), and hash cracking tools (john, hashcat). Students document their approach, tools
	Technology	
	Documentation	
Degree	% Complete (if stated)	Successfully solve CTF challenges in different categories (Linux navigation, hashing, cryptography, steganography, forensics) and submit a detailed report documenting the techniques used, commands executed, and solutions achieved, 4 hours
	% Correct (if stated)	
	Amount of Time (if stated)	
	Employability (use Montreat 360)	responsibility for assigned tasks and working together to achieve a common purpose. Critical Thinking, Think Creatively: Identify or derive alternative interpretations of data or observations, recognize new information that might support or contradict a hypothesis, explain how new information can change their understanding and ability to address a problem. Learn and Problem Solve: Ability to separate relevant and irrelevant information, integrate multiple sources of information to solve problems, and learn and apply new information to solve real-world issues

Category		Details
Name of Competency		Capture-the-Flag (CTF) Cybersecurity and Digital Forensics
Type of Activity		Capture the Flag (CTF)
Associated work role as listed in DCWF or NICE		Digital Forensics
Actor	Type of Student	An El Paso Community College student with foundational knowledge of Linux, cryptography, and forensic analysis participating in a Capture the Flag (CTF) competition
	Necessary knowledge and/or skills	
Behavior	Task The student will demonstrate cybersecurity and digital forensics skills by executing the following tasks	T1548: Determine adequacy of access controls T0167: Perform file signature analysis T0179: Perform static media analysis T1121: Decrypt seized data T1191: Determine relevance of recovered data T1322: Capture network traffic associated with malicious activities T1323: Analyze network traffic associated with malicious activities T1607: Recover information from forensic data sources
Context	Scenario	Students working teams on provided Linux machines to solve CTF challenges focused on Linux system navigation, hashing, cryptography, steganography, and basic forensic analysis. Challenges involve real-world scenarios such as decoding hidden messages, recovering deleted files, and cracking password hashes. Tools used include Linux terminal commands (e.g., find, grep, awk, strings, cat, tar), cryptographic utilities (openssl, gpg), forensic tools (binwalk, foremost, steghide), packets capture (e.g., Wireshark), and hash
	Technology	
	Documentation	

Employability

(use Montreat 360)

Teamwork. Contribute to a Common Goal: Ability to take individual responsibility for assigned tasks and working together to achieve a common purpose.

Critical Thinking, Think Creatively: Identify or derive alternative interpretations of data or observations, recognize new information that might support or contradict a hypothesis, explain how new information can change their understanding and ability to address a problem. Learn and Problem Solve: Ability to separate relevant and irrelevant information, integrate multiple sources of information to solve problems, and learn and apply new information to solve real-world issues.

Category		Details
Name of Competency		Capture-the-Flag (CTF) Cybersecurity and Digital Forensics
Type of Activity		Capture the Flag (CTF)
Associated work role as listed in DCWF or NICE		Digital Forensics
Actor	Type of Student	An El Paso Community College student with foundational knowledge of Linux, cryptography, and forensic analysis participating in a Capture the Flag (CTF) competition
	Necessary knowledge and/or skills	
Behavior	Task The student will demonstrate cybersecurity and digital forensics skills by executing the following tasks	T1548: Determine adequacy of access controls T0167: Perform file signature analysis T0179: Perform static media analysis T1121: Decrypt seized data T1191: Determine relevance of recovered data T1322: Capture network traffic associated with malicious activities T1323: Analyze network traffic associated with malicious activities T1607: Recover information from forensic data sources
Context	Scenario	Students working teams on provided Linux machines to solve CTF challenges focused on Linux system navigation, hashing, cryptography, steganography, and basic forensic analysis. Challenges involve real-world scenarios such as decoding hidden messages, recovering deleted files, and cracking password hashes. Tools used include Linux terminal commands (e.g., find, grep, awk, strings, cat, tar), cryptographic utilities (openssl, gpg), forensic tools (binwalk, foremost, steghide), packets capture (e.g., Wireshark), and hash cracking tools (john, hashcat). Students document their approach, tools used, and methodology for solving challenges.
	Technology	
	Documentation	
	Limitations	
Degree	% Complete (if stated)	Successfully solve CTF challenges in different categories (Linux navigation, hashing, cryptography, steganography, forensics) and submit a detailed report documenting the techniques used, commands executed, and solutions achieved, 4 hours
	% Correct (if stated)	
	Amount of Time (if stated)	
Employability	(use Montreat 360)	Teamwork. Contribute to a Common Goal: Ability to take individual responsibility for assigned tasks and working together to achieve a common purpose. Critical Thinking, Think Creatively: Identify or derive alternative interpretations of data or observations, recognize new information that might support or contradict a hypothesis, explain how new information can change their understanding and ability to address a problem. Learn and Problem Solve: Ability to separate relevant and irrelevant information, integrate multiple sources of information to solve problems, and learn and apply new information to solve real-world issues.

2025 CAE Community Symposium

Workforce
+
Education
=
Experiential
Learning



NCYTE
CENTER

National Cybersecurity Training & Education Center



	Thursday Nov 21	Friday Nov 22	Saturday Nov 23
	AST 307 and AST 150	AST 150	AST 150
8:00		Light Breakfast	Light Breakfast
8:30			
9:00		Welcome to the Hack the Border, Speakers	
9:30			
10:00		Adversarial Thinking Challenges	Team Presentations
10:30		Hack the Turing	
11:00		Capture the Flag Competition	
11:30			
12:00		Lunch + Keynote Speaker	Hackathon Closing Ceremony and Awards
12:30			
1:00	Registration		
1:30	Check-In		
2:00	Team Building		
2:30	Social Time		
3:00			
3:30	AST 307		
4:00	Android Exploitation Workshop		
4:30	AST 307		
5:00		Secure Coding Challenges	
5:30		Phishing Awareness	
6:00	NCyTE Industry Night Professional Panel		
6:30			
7:00	AST 150		
7:30			
8:00			



IEEE



El Paso Electric





NCYTE CENTER

National Cybersecurity Training & Education Center

Day 1: Industry Nights:
64 industry members
Private and Public Sector
Army and other agencies



Villages

November 22nd, 2024



Phishing



Hack th Turing



CTF



Adversarial Thinking



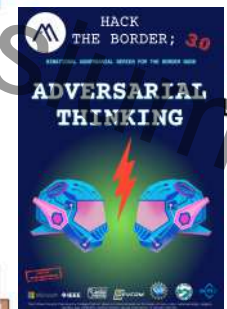
Secure Code



Datathon



Challenges



Hack the Border Video



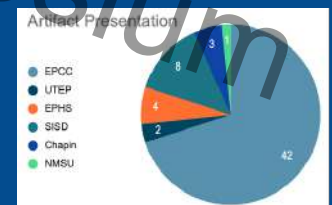
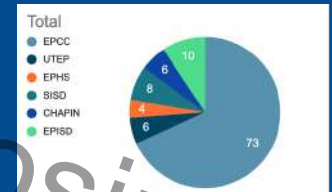
Villages



Total Participants:
107 (Friday, 22nd)

Teams Presenting Artifacts:
17 teams (60 participants) (Saturday, 23rd)

Attendees by Institution:
EPCC: 73
UTEP: 6
High Schools: 28



hacktheborder.org



**HACK
THE BORDER; 30**

BINATIONAL ADVERSARIAL SERIES FOR THE BORDER GOOD

**WORKSHOP
CRYPTOGRAPHY**

Step into the world of cyber defense!

Learn to encrypt and decrypt files like a pro and experience hack funtastic to keep your data secure.

November 3, 2024 at 4:00 pm.
 SEC W.V. Campus, RM 101
 Contact: oas@wvsec.gov
 RSVP: <https://bit.ly/hackborder>

ALS Module Are Welcome
 No Technical Experience Needed
 Limited seats available - RSVP!

Microsoft IEEE U.S. Customs and Border Protection

The Five County Community College District and its departments are the lead of various local, regional, and national organizations that are working together to support the community.

HACK

THE BORDER; 30

INTERNATIONAL ADVERTISING SERIES FOR THE BORDER BOOK

WORKSHOP

DEFENSIVE SECURE CODING

Robert Jacobson, APT

Defensive secure coding is a proactive approach to software development focused on building resilient, secure applications. Rather than merely addressing known vulnerabilities, it anticipates potential risks by embedding practices like validating inputs, managing errors, controlling data access, and securely handling sensitive information. By adopting these practices developers proactively build more secure applications that are not only functional but also secure by design, minimizing risks and ensuring greater reliability for users.

- > November 12, 2024 at 6:30 pm.
- > Contact: dev@livespcr.com
- > Online: Spoc Live!

<https://usfheeh.com/en/5793848d84772e9c56887ca9cc977ea9-1>

"I am in full support of the free use of all creative works, including digital works."

The Official Google Commonsense Copyright Office said on YouTube.com in the basis of a "zero tolerance policy".

Microsoft FHEE ACM



HACK THE BORDER; 30

BINATIONAL ADVERSARIAL SERIES FOR THE BORDER GOOD

**WORKSHOP
ADVERSARIAL THINKING**

⚡

Learn to anticipate challenges and threats from a critical perspective

⚡

Two stylized human heads made of circuitry, facing each other.

October 31, 2024 at 4:00 pm
 KRCO W.V. Campus, Rm 307
 Contact: convergencetech@hbtg.org
 RSVP: <https://hacktheborder.org>

WV Regional Executive Council
 Limited seats available - RSVP!

Microsoft | IEEE | WVU | WVU Center for Cybersecurity | WVU Center for Global Health | WVU Center for Innovation & Entrepreneurship | WVU Center for Leadership & Governance | WVU Center for Policy & Strategy | WVU Center for Social & Behavioral Science | WVU Center for the Study of the American West

HACK THE BORDER; 3.0

INTERNATIONAL ADVERSARIAL SERIES FOR THE BORDER HOOD

WORKSHOP

DRAGON CITY - PREVENTING A NUCLEAR DISASTER THROUGH CYBERSECURITY

by Gaurav Purohit Ph.D., Computer Engineering,
The U.S. Army Center of Cyber Intelligence Development Command

This hands-on workshop will immerse the participants in a journey of preventing a nuclear disaster by finding quantum information to generate a cybersecurity vector to safely turn-off a malfunctioning nuclear reactor. In addition, there will be a discussion of administrator (blue team) mitigation actions that can prevent cybersecurity breaches in the future on those IoT devices and sensors.

- > November 14, 2024 at 4:00 pm.
- > RROC V.V. Campos, ARS Sbar, Contact: ccv@npsig.edu
- > RSVP: <https://thehackborder.org>
- > All Majors Area Welcome
- > No Technical Experience Needed
- > Limited seats available - RSVP!

Sponsors: Microsoft, IEEE, GECON, ACM, and others.

The Physics Cyber Community Graduate Student Council organizes these workshops on the basis of state-of-the-art national research activities.



The poster features a central illustration of a person in a white lab coat with a stethoscope, holding a smartphone that displays a red Android robot icon. The background is dark blue with a grid pattern. At the top, the text 'HACK THE BORDER;' is in white, followed by a large red '30' with a white outline. Below this, 'INTERNATIONAL ADVERSARIAL SERIES FOR THE BORDER GOOD' is written in white. The main title 'WORKSHOP ANDROID EXPLOITATION' is in large, bold, white letters. To the left of the title, it says 'by Jonathan Martinez, @jmartinez4science, aka P.B. Army, former @qualcomm-developer @google' in white. A red-bordered box on the right contains white text describing the workshop's focus on learning techniques used by malware developers to exploit Android applications, designed for an intermediate audience, covering concepts like the Android OS, the Dalvik VM, and the AndroidManifest.xml file, and mentioning a Q&A session and a certificate of completion. To the right of the illustration, the date and time 'November 11, 2024 at 4:00 pm' are listed, along with the location 'Hack U.V. Campus, AED 360', contact information 'Contact: acaevall@secops.edu', and the RSVP link 'RSVP: <https://hacktheborder.org>'. Below the illustration, a red-bordered box contains the text 'All Major Areas Welcome', 'No Technical Experience Needed', and 'Limited seats available - RSVP!'. At the bottom, logos for Microsoft, IEEE, Qualcomm, Google, and ACM are displayed, along with the text 'The IEEE Texas County Community College District does not discriminate on the basis of race, color, national origin, gender, age, disability, or sexual orientation.' and '© 2024 IEEE'.

HACK THE BORDER; 30

INTERNATIONAL ADVERSARIAL SERIES FOR THE BORDER GOOD

WORKSHOP
ANDROID EXPLOITATION

by Jonathan Martinez, @jmartinez4science,
aka P.B. Army, former @qualcomm-developer @google

Learn the techniques used by malware developers to exploit Android applications. These applications are designed to gain control and access sensitive user data & violate the security using an API file. The workshop will show how these techniques are used like the **AndroidManifest.xml** file by explaining common security measures and offer real-world look into the device.

November 11, 2024 at 4:00 pm
Hack U.V. Campus, AED 360
Contact: acaevall@secops.edu
RSVP: <https://hacktheborder.org>

All Major Areas Welcome
No Technical Experience Needed
Limited seats available - RSVP!

Microsoft | IEEE | Qualcomm | Google | ACM

The IEEE Texas County Community College District does not discriminate on the basis of race, color, national origin, gender, age, disability, or sexual orientation.

© 2024 IEEE

2025 CAE



Page 4 West Texas County Courier December 5, 2024

Hack the Border 3.0

EPCC, national sponsors, host tech conference

By Beau Bagley
Special to the Courier

EL PASO COUNTY – El Paso Community College computing fields of study (Computer Science, Cybersecurity, and Artificial Intelligence Analytics) hosted the nationally renowned 3rd Annual 'Hack the Border 3.0', an event that offered workshops in Artificial Intelligence and Cybersecurity, along with competitions like 'Capture the Flag' (CTF), Adversarial Thinking, Phishing, Secure Coding, and the first 'Dataathon'.

EPCC is designated as a Center of Academic Excellence in Cybersecurity and has garnered attention from organizations such as NCYTE and the NSA. Notably, the NSA has highlighted the use of experiential learning in cybersecurity subject matter.

Sponsors of the event include: El Paso Electric, Microsoft, National Science Foundation (NSF), The U.S. Army Corps of Engineers Development Command (DEVCOM), National Cybersecurity Training & Education Center (NCYTE), Association of Computing Machinery (ACM), and the Institute of Electrical and Electronics Engineers (IEEE).

"This sense of belonging – feeling accepted, valued, and connected – helps students understand their role within the community and the relevance of their contributions," Dr. Christian Servin, EPCC Computer Science Professor and Hack the Border Co-Founder, with Instructor Nadia Karichev, said. "Hack the Border aims to cultivate this feeling, which is essential for building self-esteem, motivation, and engagement, ultimately empowering students to thrive in both their personal and professional lives."

A key highlight of Hack the Border 3.0 is the introduction of our first Dataathon, generously sponsored by El Paso Electric. Now a permanent feature of the program, this Dataathon offered students in fields like data analytics, health informatics, and other informatics disciplines a chance to apply and refine their skills through real-world challenges that benefit the community. El Paso Electric has provided a comprehensive dataset reflecting local data, allowing students to engage with issues that impact their community and foster a sense of belonging through meaningful problem-solving.

CTF competitions provide hackathon participants with an opportunity to engage in hands-on scenarios and apply solutions based on the knowledge and skills they have acquired through training or education. The CTF challenges we offer extend concepts and topics identified by our regional industry partners as critical needs.

On Thursday, November 21, 2024, EPCC hosted "Industry Nights," bringing together regional industry leaders and workforce representatives to discuss valuable credentialing opportunities and explore ways to enhance curricula.



Dr. Christian Servin



PROBLEM SOLVING – Chao Schwan, left, and Josepina Lopez work on a hack.

helping students understand regional workforce needs and access work-based learning opportunities. This initiative is supported by the National Cybersecurity Training & Education Center (NCYTE) and featured two distinguished speakers: Stephen Miller, Principal Investigator for NCYTE, and Michelle Lamhart from the National Security Agency (NSA).

Additionally, as J.J. Childress from Microsoft attested, EPCC was recently mentioned in national news for its role in Hack the Border. This recognition underscores the national impact we are making.

In addition, DEVCOM, our official sponsor for "adversarial thinking," offered exceptional workshops that integrate AI and cybersecurity. Through the support of a Microsoft grant, we are building capacity in artificial intelligence tools and technology, with both DEVCOM and NCYTE helping us expand these resources for students, the workforce, and city leaders.

This project would not have been possible without the extraordinary efforts of the Hack the Border team. Karichev's leadership was instrumental in overseeing the coaching component of the hackathon. Her preparation and training of coaches ensured the successful integration of relevant challenges into the event.

Isaac Proxa, Andrew Ponomik, and Rafael Escalante provided invaluable contributions in designing the challenges and platforms that fostered a dynamic and engaging hackathon environment.

The event's success also depended on the dedicated coaches – Jesus Ramirez, Louis Dominguez, Victor Razo, Sirach Mejia, Saul Macias, Delilah Espanza, Armando Levario, Alejandro Salano, and Ivan Alonso.



Year	Event	Location	Coaches
2024	Hack the Border 3.0	EPCC	Jesus Ramirez, Louis Dominguez, Victor Razo, Sirach Mejia, Saul Macias, Delilah Espanza, Armando Levario, Alejandro Salano, Ivan Alonso
2023	Hack the Border 2.0	EPCC	Jesus Ramirez, Louis Dominguez, Victor Razo, Sirach Mejia, Saul Macias, Delilah Espanza, Armando Levario, Alejandro Salano, Ivan Alonso
2022	Hack the Border 1.0	EPCC	Jesus Ramirez, Louis Dominguez, Victor Razo, Sirach Mejia, Saul Macias, Delilah Espanza, Armando Levario, Alejandro Salano, Ivan Alonso
2021	Hack the Border 0.0	EPCC	Jesus Ramirez, Louis Dominguez, Victor Razo, Sirach Mejia, Saul Macias, Delilah Espanza, Armando Levario, Alejandro Salano, Ivan Alonso



Thank You For Your Attention

Christian Servin, Ph.D.
cservin1@epcc.edu
El Paso Community College
ITS/Computer Science Program



Acknowledgments

Partial support for this work was provided
by the National Science Foundation
under grant DUE-2300378.



EPCC's National Center of Academic
Excellence in Cyber Defense