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

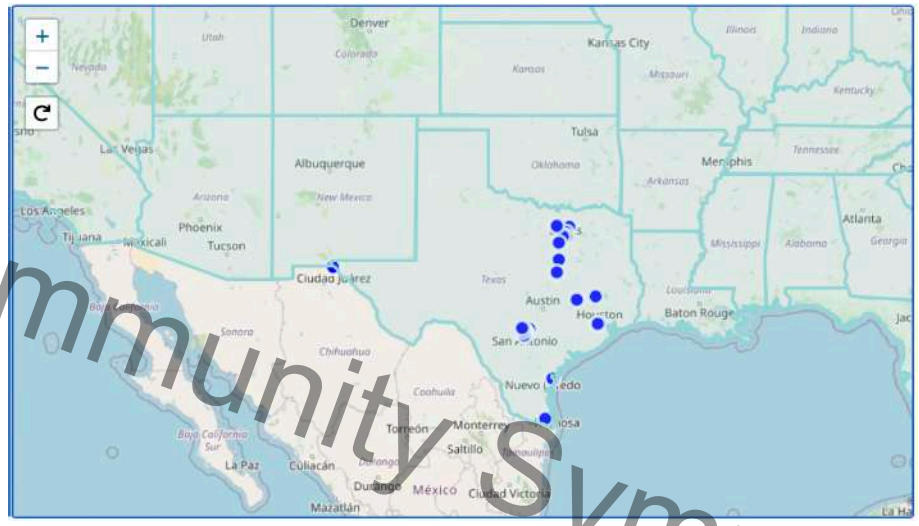
Introduction/ Background

- **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.

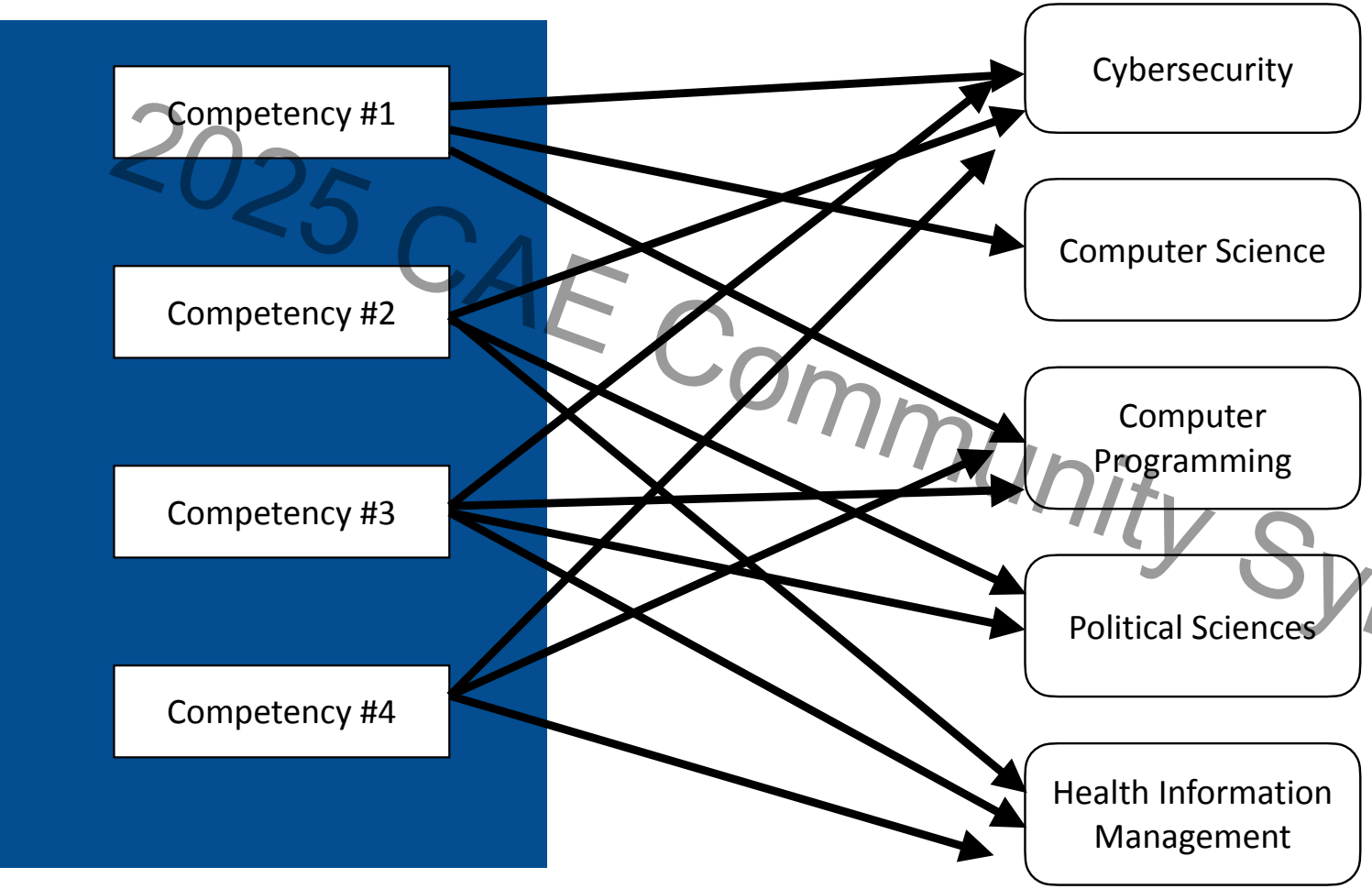
About Project

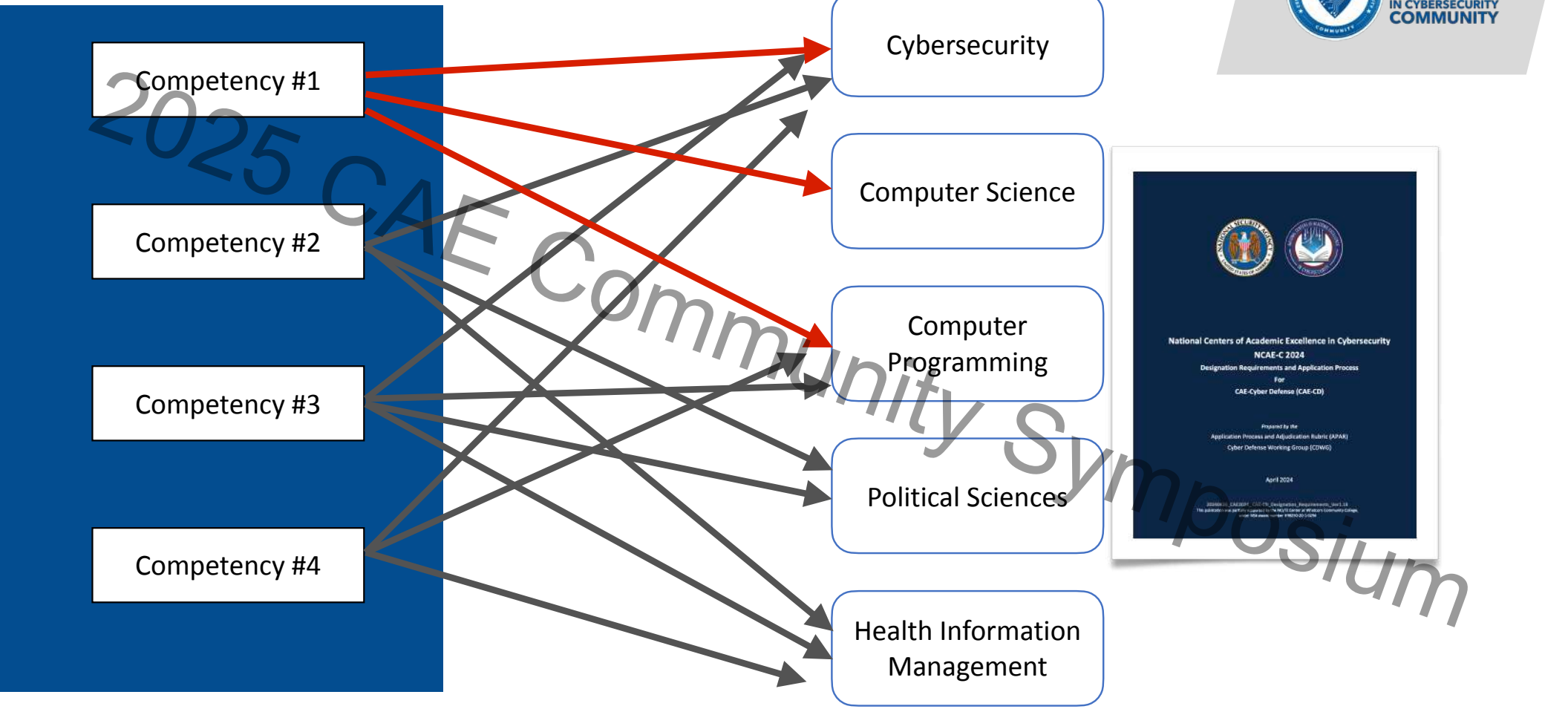
- **Experiential Learning as a Solution**
  - Hackathons, CTF competitions, and national challenges address competency gaps.
  - These activities provide hands-on experience but face logistical and institutional barriers.
- **Proposed Hackathon Framework**
  - Based on the Essential Elements (ABCDE) 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.

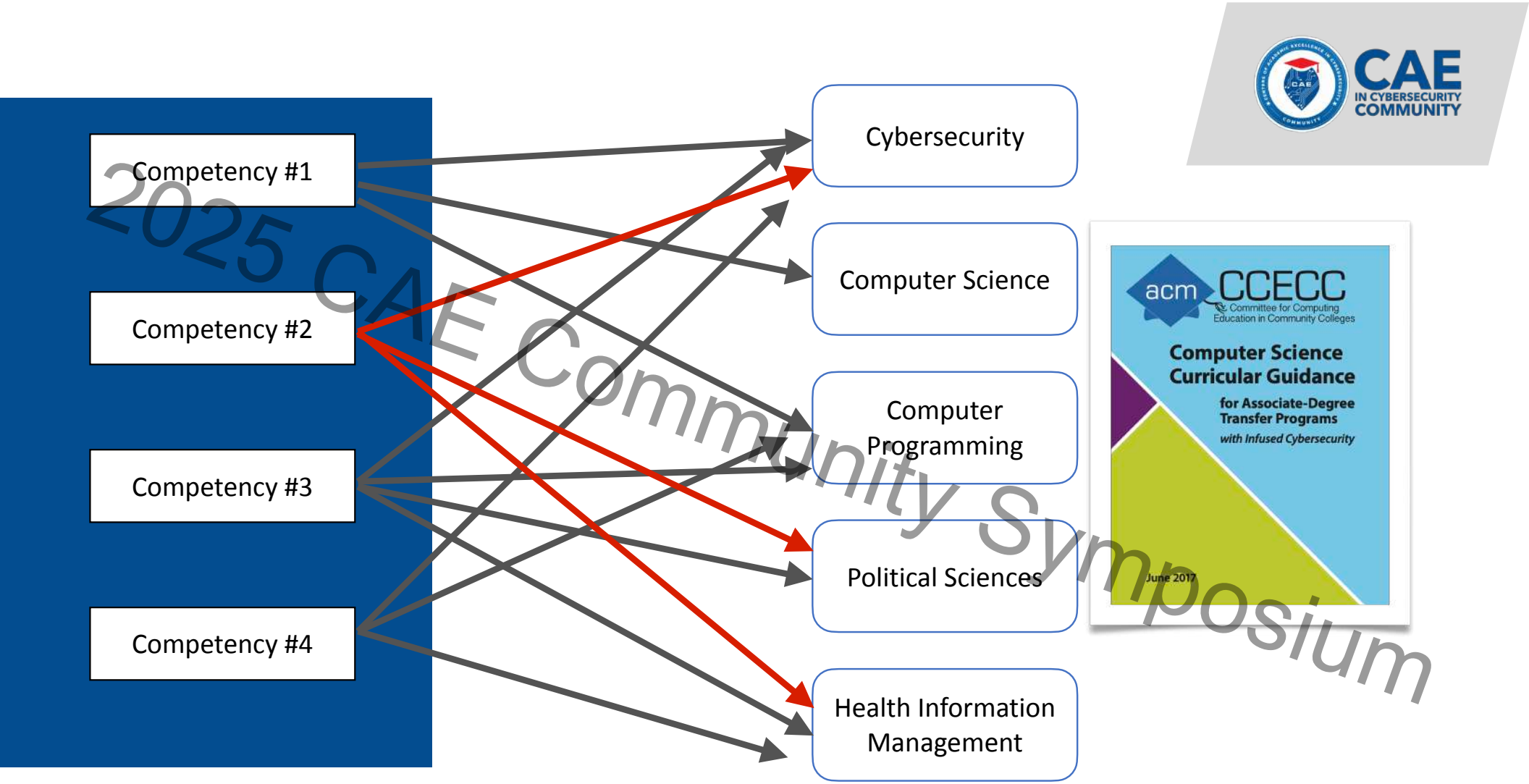
- **Borderplex Region**: Serves 2.5M people, the largest bilingual & binational workforce.
- **HSI**: 85%+ Hispanic students (EPCC 2020).
- **Location:** Near Fort Bliss, White Sands, 500 miles from Dallas & Houston.
- **Education:** 18 Dual Credit, 18 ECHS, 19 P-TECH programs.
- **STEM**: 2+2 MOU, including 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.

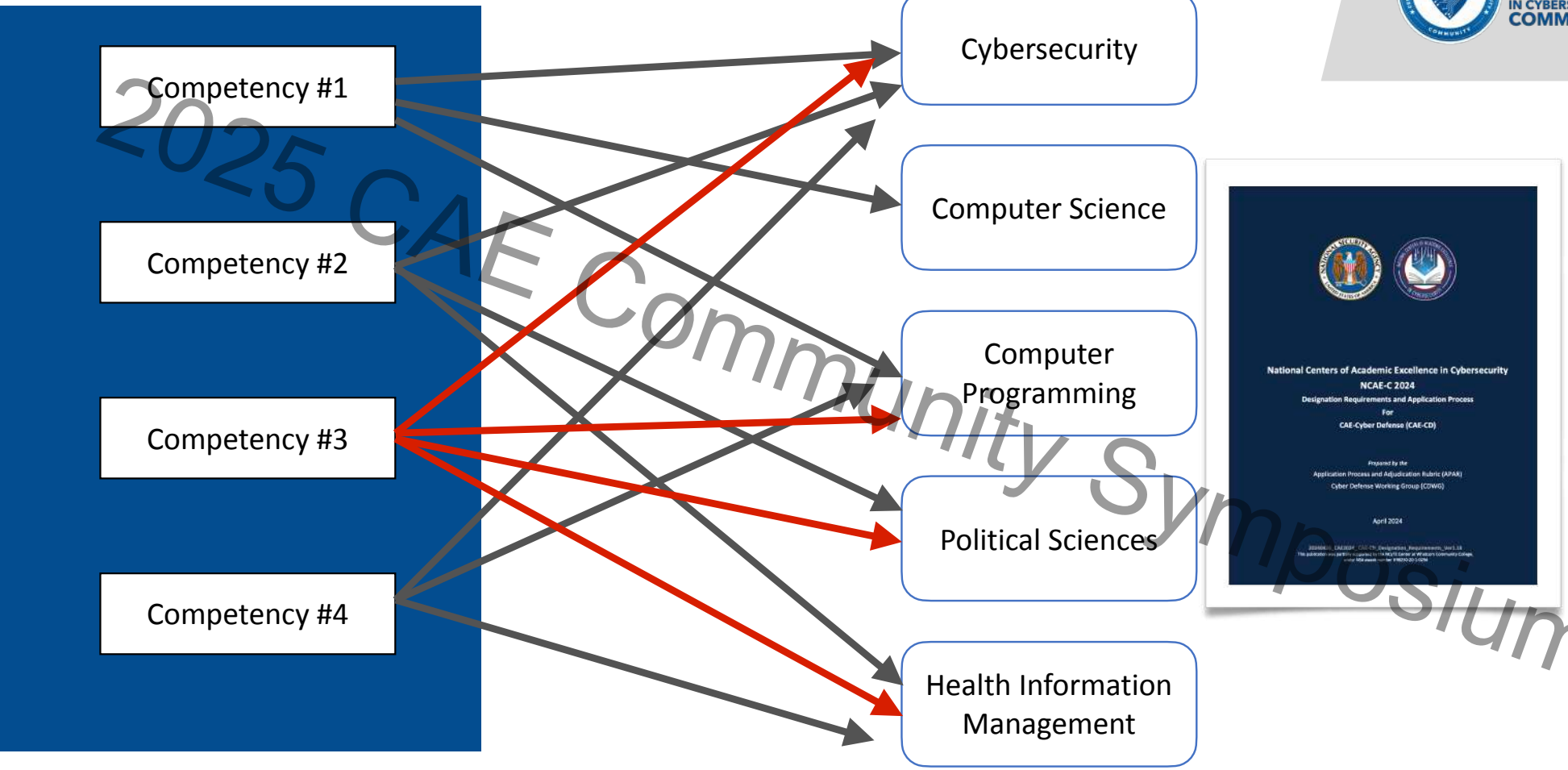


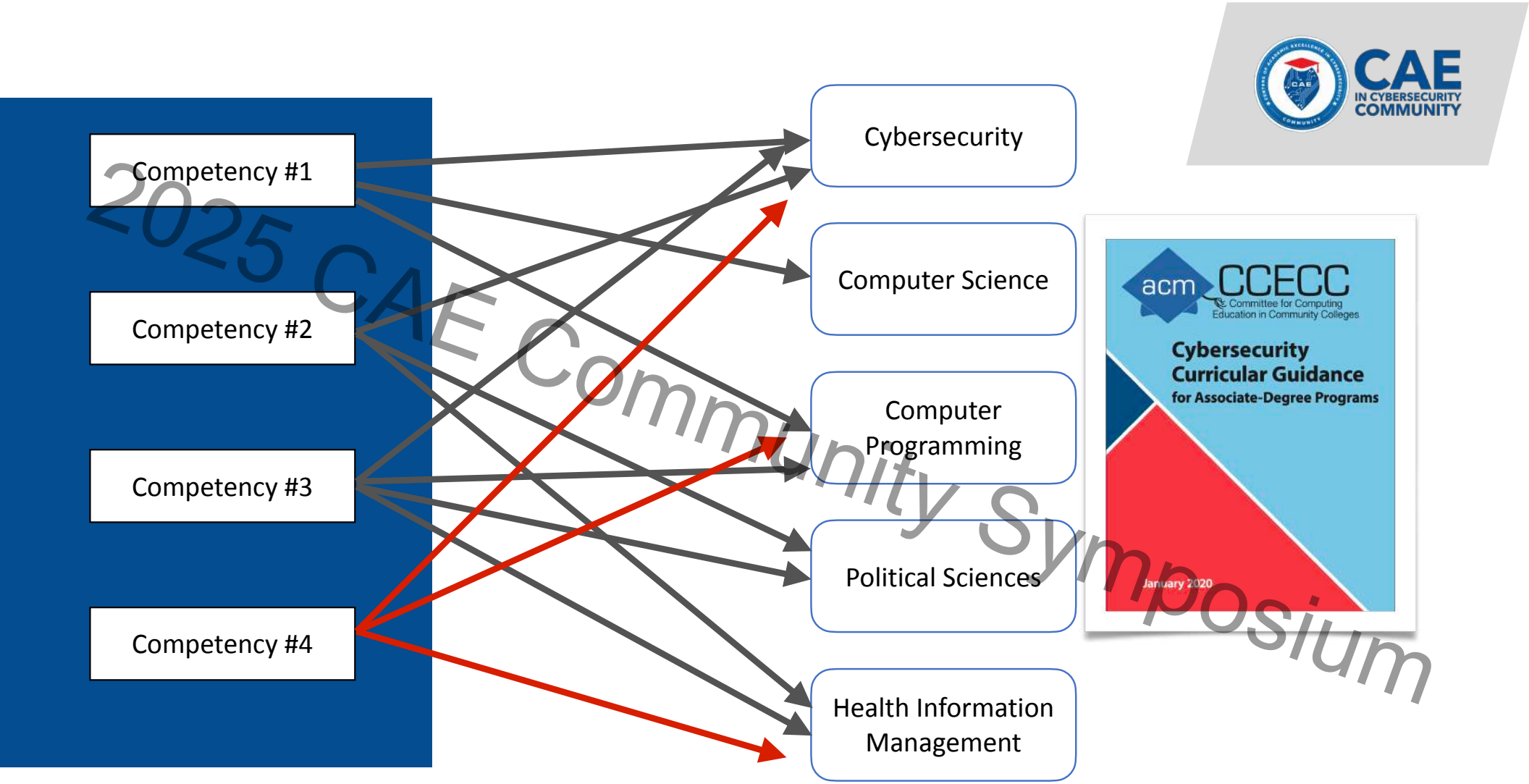
26 Institutions in Texas

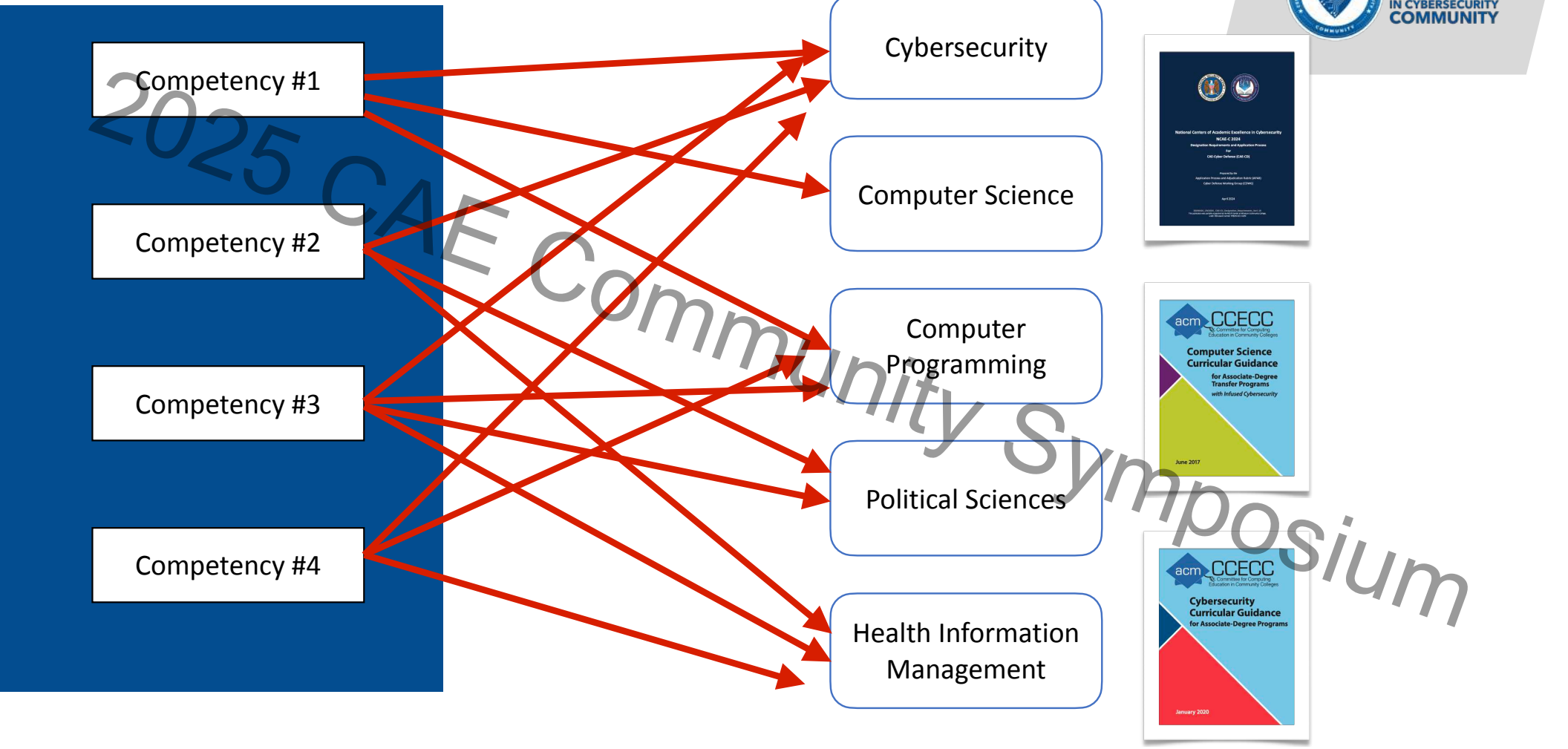












DEFINITION AND 5 ESSENTIAL ELEMENTS

"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 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
	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 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
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)	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 Necessary knowledge and/or skills	An El Paso Community College student with foundational knowledge of Linux, cryptography, and forensic analysis participating in a Capture the Flag (CTF) competition
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 Technology Documentation	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
Degree	% Complete (if stated) % Correct (if stated) Amount of Time (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
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

Workforce
+
Education
=
Experiential
Learning

2025 CAE Community Symposium

NCyTE CENTER
National Cybersecurity Training & Education Center

CAE IN CYBERSECURITY COMMUNITY

	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 / Hack the Turing / Capture the Flag Competition	Team Presentations
10:30			
11:00			
11:30			
12:00		Lunch + Keynote Speaker	
12:30			Hackathon Closing Ceremony and Awards
1:00			
1:30	Registration Check-In Team Building Social Time AST 307	Datathon	
2:00			
2:30			
3:00			
3:30			
4:00	Android Exploitation Workshop AST 307	Secure Coding Challenges / Phishing Awareness / Hack the City	
4:30			
5:00			
5:30	NCyTE Industry Night Professional Panel AST 150		
6:00			
6:30			
7:00			
7:30			
8:00			

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

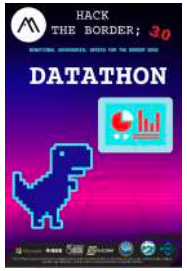
Hack th Turing

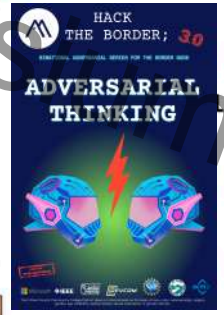
CTF

Adversarial Thinking

Secure Code

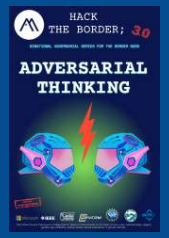
Datathon

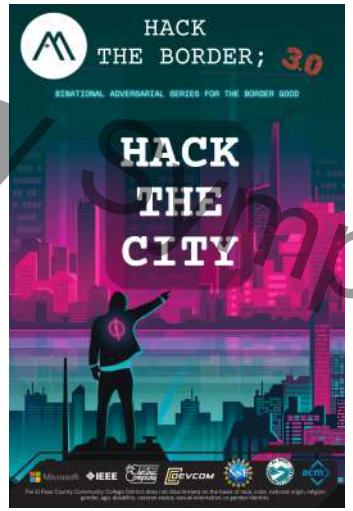




Hack the Border Video

Villages



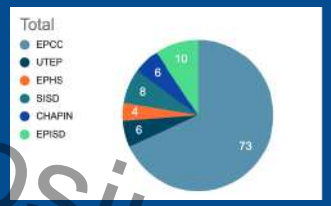


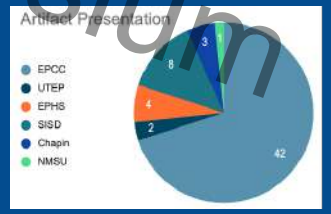
CAE IN CYBERSECURITY COMMUNITY

Total Participants:
107 (Friday, 22nd)

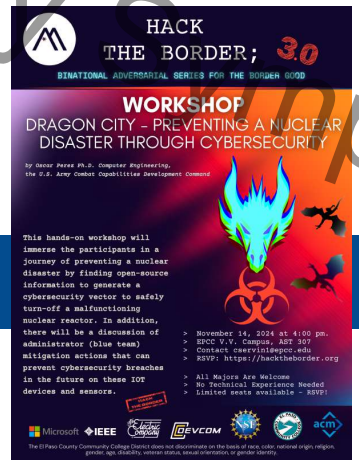
Teams Presenting Artifacts:
17 teams (60 participants) (Saturday, 23rd)

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





hacktheborder.org



2025 CAE Community Symposium

1973 51 Years 2024

West Texas County COURIER

VOL. 51, No. 49 — Serving Anthony, Vinton, Canutillo, East Montana, Horizon, Socorro, Clint, San Elizario and Tornillo — DECEMBER 5, 2024

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 'Datathon'.

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 our use of experiential learning in cybersecurity as a best practice.

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

Dr. Christian Servin

"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 Datathon, generously sponsored by El Paso Electric. Now a permanent feature of the program, this Datathon 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, 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 Isenhart from the National Security Agency (NSA).

Photo courtesy El Paso Community College

PROBLEM SOLVING – Chad Schaar, left, and Josephine Lopez work on a hack.

Additionally, as J.J. Childress from Microsoft shared, 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 Perea, Andrew Pownuk, 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, Raul Macias, Delilah Esparza, Armando Levario, Alejandro Solano, and 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