Bridging the Divide: Mapping Hands-on Labs to Cybersecurity Competency Statements

Ayad Barsoum, Ph.D
Director of NSA/DHS Designated Center for Cyber Excellence
St. Mary's University, San Antonio, Texas

Meet the need

- Collaboration with local companies
- Skills required by industry professionals
- Align the curriculum with real-world demands

ABCDE model

- Aligning hands-on labs
- Integration of hands-on labs into competency statements
- Example: Buffer overflow vulnerabilities

Buffer overflow vulnerabilities

ABCDE Model	Attributes ABCDE	Value
Actor	Actor	Cybersecurity students taking a 600-level Computer Security & Privacy course
	Description	Completed introductory computer programming courses
Behavior	Work role	Software Developer
	Task	T0046: Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.
	Task details	Students receive multiple C programs containing buffer overflow vulnerabilities. Their task is to identify these vulnerabilities and implement the necessary fixes.

Buffer overflow vulnerabilities

Condition/Context	Scenario	Students are provided with multiple C programs designed to perform distinct tasks: a) authenticate users based on passwords; b) copy buffers between memory locations; c) read a chunk of data from a file to a memory buffer. However, these programs, written in C language, include buffer overflow vulnerabilities. Students are challenged to identify these vulnerabilities and subsequently rectify them by rewriting the programs to achieve the desired results in a secure manner.
	Limitations	Rewrite the programs in C language (avoiding the use of any other programming languages)
	Technology	Visual Studio (or other IDE that supports C compilers)
	Documentation	Security Development Lifecycle (SDL) Banned Function Calls

Buffer overflow vulnerabilities

Degree	Complete	Identify a minimum of three buffer vulnerabilities in the provided program and offer recommendations for their resolution
	Correct	Successfully implement fixes for the identified buffer overflow vulnerabilities
	Time	60 minutes
Employability		Students enhance problem-solving skills, critical thinking, and programming proficiency


2024 CAE Community Symposium
Thank you