

How Dr. Pedro Diaz-Gomez Brings Cybersecurity to Life Through **ACI Skill Labs**

For more than a decade, **Dr. Pedro Diaz-Gomez** has designed his cybersecurity courses around a simple but powerful principle:

Theory and practice are inseparable.

As a professor of cybersecurity, Dr. Diaz-Gomez believes students learn best when they first understand the underlying concepts and then immediately apply them in realistic environments. His philosophy has shaped every course he teaches, from Computer Security to Network Security, where hands-on experience is not an optional supplement—it is an essential part of the learning process.



Pedro Diaz-Gomez
Cyber Security Professor

“

I consider myself a professor of practice. There is no better theory without practice, and there is no good practice without theory. Those two things go hand in hand.

”

For over ten years, Dr. Diaz-Gomez has **incorporated ACI Skill Labs into his courses**, making laboratory exercises a central component of student learning. Today, laboratory work represents approximately 40% of the final course grade, reinforcing the importance of developing practical skills alongside conceptual understanding.



The Challenge:

Transforming Theory into Professional Skills

Cybersecurity is an applied discipline. While students must understand concepts such as access control, malware analysis, authentication, denial-of-service attacks, and network security, simply reading about these topics is not enough.

"If I don't have labs, then my course becomes too theoretical," says Dr. Diaz-Gomez.

Students preparing for careers in cybersecurity must configure Active Directory, analyze malware behavior, investigate security events, and execute the same commands they will encounter in professional environments. Understanding why a technology works is essential—but so is knowing how to use it.

“

Professionally, I think the skills the students gain are tremendous.

”



The Solution:

A Curriculum Where Theory and Practice Reinforce Each Other

Rather than assigning generic laboratories, Dr. Diaz-Gomez carefully maps each Skill Lab to the concepts being covered in class. Every laboratory is intentionally selected from the ACI Skill Labs catalog to reinforce the week's lecture material.



The correspondence between the theory and the labs is beautiful. If I am teaching access control and authentication, students are working with Active Directory. If I am discussing malware, they are analyzing malware in the lab. If we study denial-of-service attacks, they perform exercises directly related to denial-of-service.



This close alignment allows students to immediately apply newly learned concepts, strengthening both their theoretical understanding and practical competence.

The course structure is equally deliberate. At the beginning of every semester, students receive the complete laboratory schedule, identifying which labs correspond to each week of instruction. This organization provides transparency, encourages students to work ahead when appropriate, and establishes clear expectations from the very first day of class.

"The freedom they have is important. They know the schedule in advance. They can work ahead if they choose, and the course is easy to follow."

The laboratories also serve as the foundation for larger programming and security projects. Students frequently build automation tools in Python based on procedures they first performed manually during the labs. In this way, laboratory exercises are not isolated activities but become building blocks for increasingly sophisticated cybersecurity tasks.



Results:

Building Confidence Through Experience

Many students begin Dr. Diaz-Gomez's courses with limited cybersecurity experience. The laboratories bridge the gap between classroom concepts and real-world practice by allowing students to work with professional tools and technologies in a safe learning environment.

Instead of simply recognizing security terminology, students develop the confidence to configure systems, investigate security incidents, and solve realistic cybersecurity problems.

By combining conceptual instruction with carefully integrated laboratory experiences, students leave the course with both a stronger theoretical foundation and practical skills directly applicable to the cybersecurity workforce.



Looking Ahead

Preparing Students for the Future of Cybersecurity

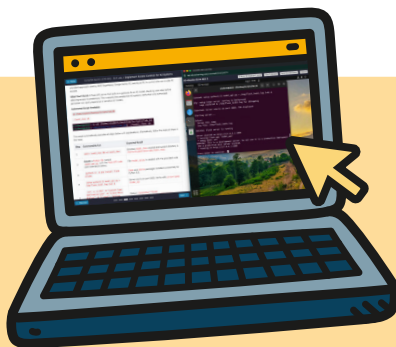
As cybersecurity continues to evolve, Dr. Diaz-Gomez believes laboratory education must evolve as well. Artificial Intelligence is rapidly becoming part of modern cybersecurity operations, and he sees AI-assisted workflows as a natural extension of future laboratory experiences.

After more than a decade of integrating Skill Labs into his teaching, Dr. Diaz-Gomez remains convinced that effective cybersecurity education requires a balance between knowledge and experience.

“

Artificial Intelligence shouldn't be treated as a novelty. It is becoming part of the way cybersecurity professionals work, and our students should learn to use it responsibly as part of their education.

”



Not using Skill Labs?

[Get Access](#)

See It In Action

[Take the Tour](#)