UF | Herbert Wertheim College of Engineering
UNIVERSITY of FLORIDA

Engineering Education Department

Enterprise Security

Course Walkthrough

Cheryl Resch

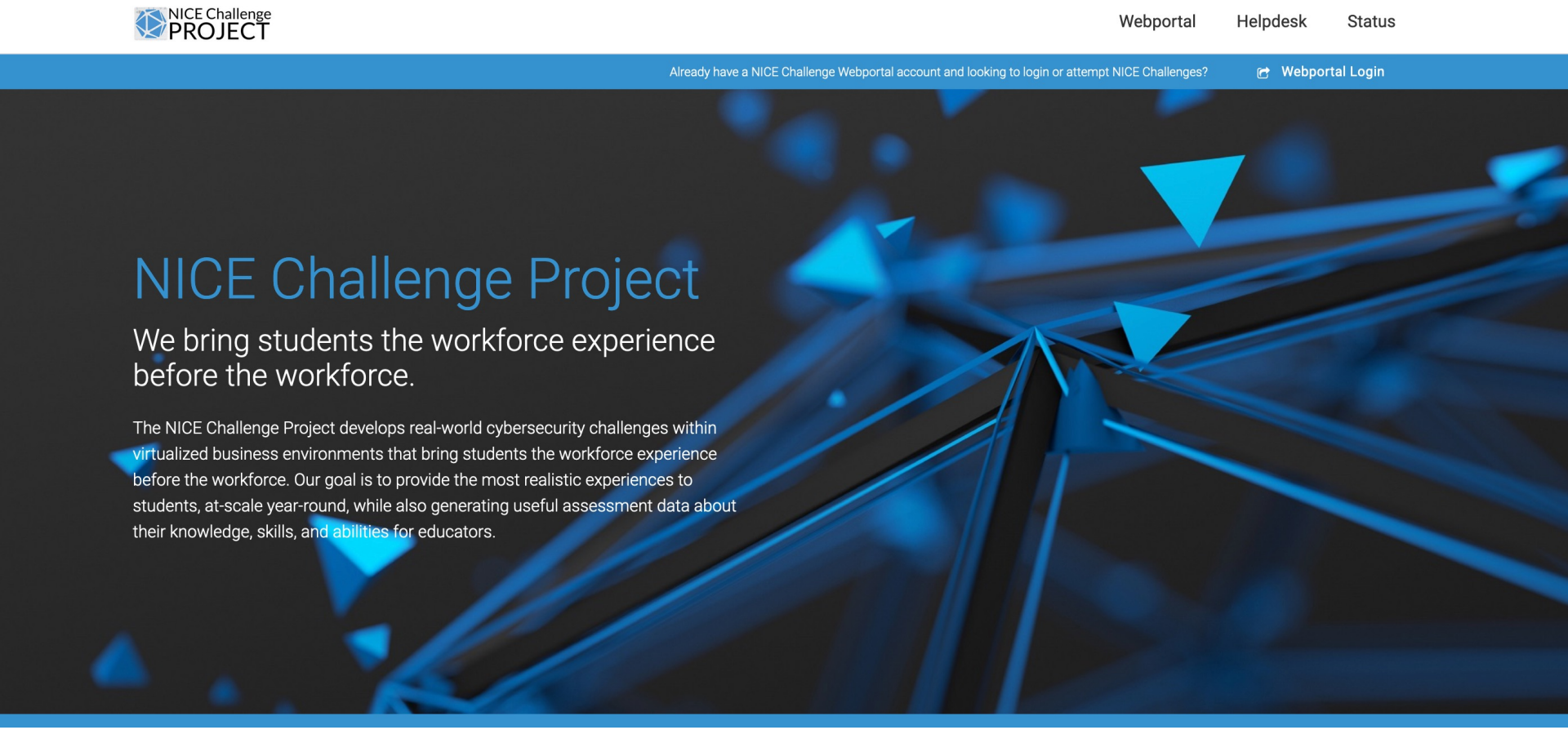
Course Description and Objectives

- Provides an introduction to the real-world aspects of defending an enterprise network. Students will gain hands-on experience performing system security tasks and handling incidents. The class begins with a basic introduction to enterprise cybersecurity, the attack sequence, and managing cybersecurity. Then lecture, homework and lab activities cover the center for internet security's twenty essential security controls.
- By the end of the semester, students should be able to
  - Identify and think critically about weaknesses in an enterprise network
  - Assess risk and prioritize problem areas
  - Identify controls to mitigate risk

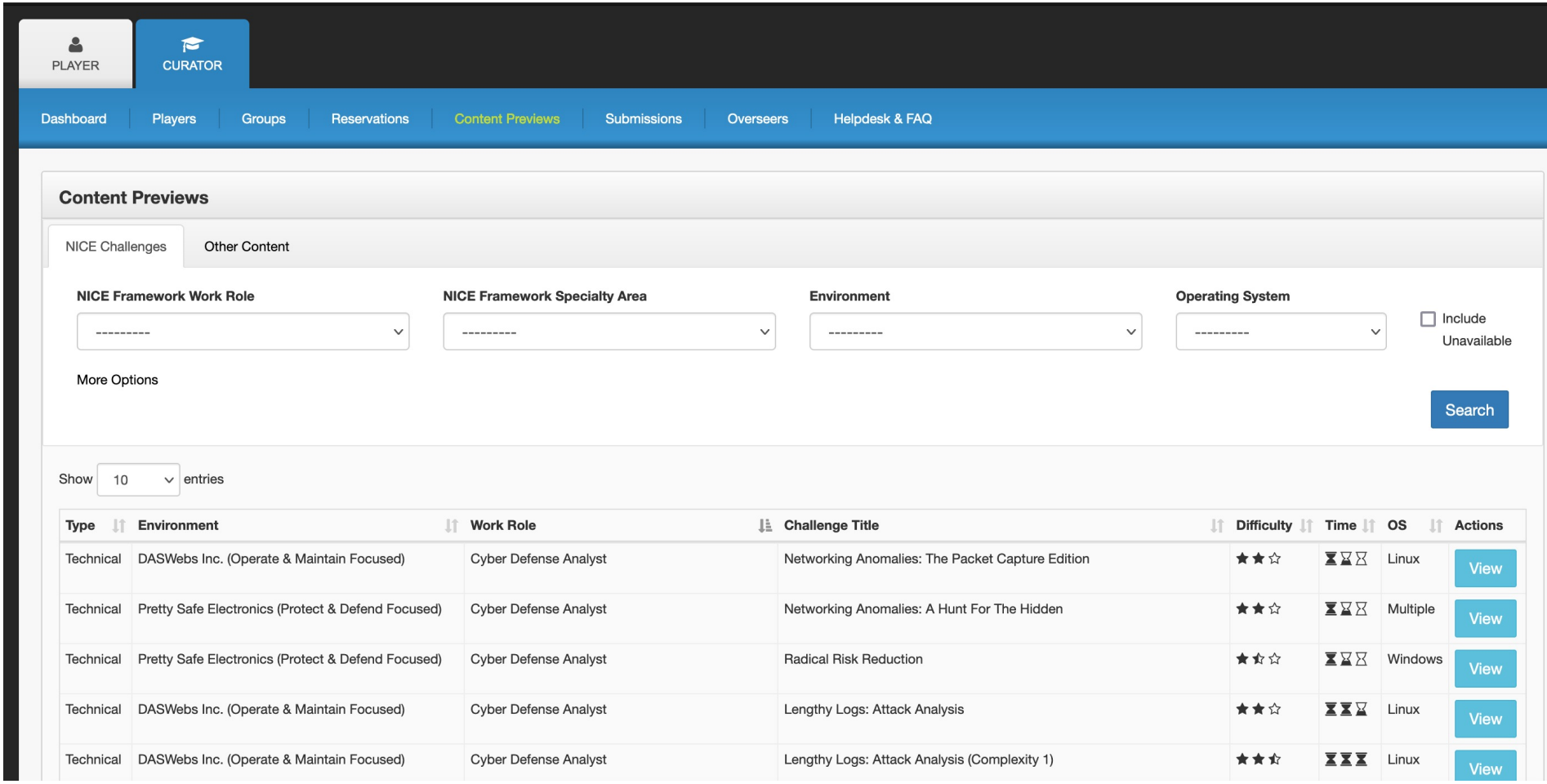
Assessments

- Labs (13) 50%
  - Weekly NICE Challenge Labs
- Homeworks (5) 15%
  - Problem sets
- Discussions (5) 15%
  - Mostly focused on products and tools
- Paper 20%
  - Design security architecture for an enterprise

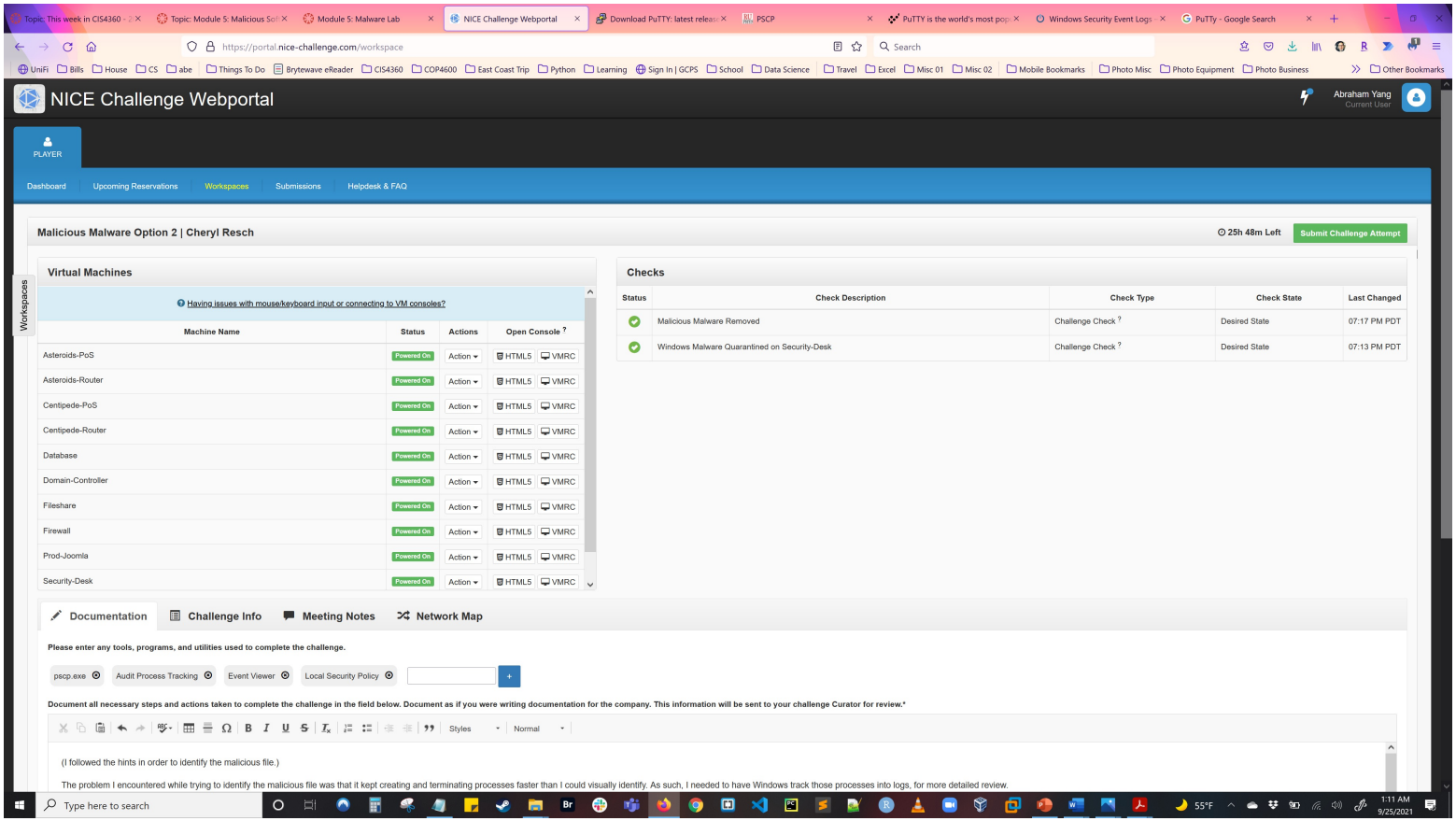
NICE Challenge Labs



NICE Challenge Labs



NICE Challenge Labs



NICE Labs Matched to Weekly Topic

- Week 1 – Cyber Security Functional Areas
- Week 2 – Risk Analysis
  - NICE Lab - ”Radical Risk Reduction”
- Week 3 – Cybersecurity Attack Sequence
  - NICE Lab - “Malicious Malware”

CIS Controls

- After week three, each class week is dedicated to one or more of the CIS Controls

Home • CIS Controls • The 18 CIS Controls

The 18 CIS Controls

Along with simplifying the Controls in v8, we've simplified the name to the "CIS Controls": Formerly the SANS Critical Security Controls (SANS Top 20) and the CIS Critical Security Controls, the consolidated Controls are now officially called the CIS Controls.

CIS Controls Version 8 combines and consolidates the CIS Controls by activities, rather than by who manages the devices. Physical devices, fixed boundaries, and discrete islands of security implementation are less important; this is reflected in v8 through revised terminology and grouping of Safeguards, resulting in a decrease of the number of Controls from 20 to 18.

Click on the individual CIS Control for more information:

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 3: Data Protection

CIS Control 4: Secure Configuration of Enterprise Assets and Software

CIS Control 5: Account Management

CIS Controls

Download CIS Controls v8

Resources and Tools

Learn about Implementation Groups

CIS Controls® Community

Join a Community

CIS Controls v7.1 is still available
Learn more about CIS Controls v7.1

NICE Labs Matched to Weekly Topic

- Week 1 – Cyber Security Functional Areas
- Week 2 – Risk Analysis
  - NICE Lab - ”Radical Risk Reduction”
- Week 3 – Cybersecurity Attack Sequence
  - NICE Lab - “Malicious Malware”
- Week 4 – Inventory and Control of Enterprise/Software Assets
  - NICE Lab – “Assuring Accurate Asset Inventories”
- Week 5 – Continuous Vulnerability Management
  - NICE Lab – “ Vulnerability scan complete, begin system hardening”
- Week 6 – Access Control Management
  - NICE Lab – “Secure Roots: Domain Organization and Access Control”
- Week 7 – Secure Configuration of Enterprise Assets and Software
  - NICE Lab – Raising the Stakes: Security by the Book”

NICE Labs Matched to Weekly Topic

- Week 8 - Audit Log Management
  - NICE Lab "Legitimate Logging Logistics"
- Week 9 - Email and Web Browser Protections
  - NICE Lab "Malicious Mail Management"
- Week 10 – Network Infrastructure Management / Network Monitoring and Defense
  - NICE Lab "Firewall Update: Tables for Two"
- Week 11 – Data Protection
  - NICE Lab "Data Backup and Recovery, Definitely Worth Testing"
- Week 12 – Account Management
  - NICE Lab "Networking Anomalies: Policy Control"
- Week 13 – Security Awareness and Training
  - NICE Lab "Dangerous Drives"
- Week 14 – Incident Response Management
  - NICE Lab "Malware Aftermath Cleanup"

Paper

- Choose an enterprise.
  - Examples are a university, a company, a county government, an office.
  - Ideally, choose a real enterprise that you are familiar with or that someone you know is familiar with.
  - Design security for this enterprise.
  - Interview people who work in this enterprise to get insight into their security needs.
  - Research the security needs of this type of enterprise.

Paper

- The paper must include:
  - Introduction - Describe the enterprise. What industry sector is it in? How large is the enterprise? Brief description of operations.
  - Asset inventory - what are the assets of this enterprise? Which are the most important assets? What is the level of confidentiality, integrity and availability required for each asset?
  - User groups and access control - Describe user groups. What data has limited access and which groups have access to it?
  - Risk analysis - Postulate threat agents who wish to harm the assets of the enterprise. Postulate actions they could take. Estimate likelihood.
  - Security control selection - For the risks laid out in the risk analysis section, describe security controls to mitigate those risks. Use CIS 18 controls as guidance, or another framework if you prefer.
- Students worked in groups of 2 or 3

- Enterprises studied included
  - UF Enterprises
    - UF Rec Sports
    - UF Gator Dining Services
    - The Agency at UF (Student run advertisement and public relations)
  - Local government agencies
    - Alachua County Public Schools
  - Small Businesses
    - UPS Store
    - Chik-fil-A franchise
  - Regional Businesses
    - Panther Medical (medical supplies distributor)
    - Synergy Technologies (IT firm)
    - InfoTech (software company)
    - Mindray Medical International (medical device manufacturer)
  - Large Corporations
    - Aerospace Corporation
    - Saudi Aramco

- Enterprises studied included
  - UF Enterprises
    - UF Rec Sports
    - UF Gator Dining Services
    - The Agency at UF (Student run advertisement and public relations)
  - Local government agencies
    - Alachua County Public Schools
  - Small Businesses
    - UPS Store
    - Chik-fil-A franchise
  - Regional Businesses
    - Panther Medical (medical supplies distributor)
    - Synergy Technologies (IT firm)
    - InfoTech (software company)
    - Mindray Medical International (medical device manufacturer)
  - Large Corporations
    - Aerospace Corporation
    - Saudi Aramco


Thank you!