



Herbert Wertheim  
College of Engineering  
UNIVERSITY of FLORIDA

Engineering Education  
Department

# Enterprise Security Course Walkthrough

Cheryl Resch

POWERING THE NEW ENGINEER TO TRANSFORM THE FUTURE

# 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

[Webportal](#)[Helpdesk](#)[Status](#)

Already have a NICE Challenge Webportal account and looking to login or attempt NICE Challenges?

[Webportal Login](#)

## NICE Challenge Project

We bring students the workforce experience before the workforce.

The NICE Challenge Project develops real-world cybersecurity challenges within virtualized business environments that bring students the workforce experience before the workforce. Our goal is to provide the most realistic experiences to students, at-scale year-round, while also generating useful assessment data about their knowledge, skills, and abilities for educators.

# NICE Challenge Labs

PLAYER

CURATOR

Dashboard
Players
Groups
Reservations
Content Previews
Submissions
Overseers
Helpdesk & FAQ

### Content Previews

NICE Challenges

Other Content

NICE Framework Work Role

NICE Framework Specialty Area

Environment

Operating System

Include Unavailable

More Options Search

Show  entries

Type	Environment	Work Role	Challenge Title	Difficulty	Time	OS	Actions
Technical	DASWebs Inc. (Operate & Maintain Focused)	Cyber Defense Analyst	Networking Anomalies: The Packet Capture Edition	★★☆	⌚⌚⌚	Linux	<a href="#" style="background-color: #00a6c9; color: white; padding: 2px 5px; border-radius: 5px;">View</a>
Technical	Pretty Safe Electronics (Protect & Defend Focused)	Cyber Defense Analyst	Networking Anomalies: A Hunt For The Hidden	★★☆	⌚⌚⌚	Multiple	<a href="#" style="background-color: #00a6c9; color: white; padding: 2px 5px; border-radius: 5px;">View</a>
Technical	Pretty Safe Electronics (Protect & Defend Focused)	Cyber Defense Analyst	Radical Risk Reduction	★★☆	⌚⌚⌚	Windows	<a href="#" style="background-color: #00a6c9; color: white; padding: 2px 5px; border-radius: 5px;">View</a>
Technical	DASWebs Inc. (Operate & Maintain Focused)	Cyber Defense Analyst	Lengthy Logs: Attack Analysis	★★☆	⌚⌚⌚	Linux	<a href="#" style="background-color: #00a6c9; color: white; padding: 2px 5px; border-radius: 5px;">View</a>
Technical	DASWebs Inc. (Operate & Maintain Focused)	Cyber Defense Analyst	Lengthy Logs: Attack Analysis (Complexity 1)	★★☆	⌚⌚⌚	Linux	<a href="#" style="background-color: #00a6c9; color: white; padding: 2px 5px; border-radius: 5px;">View</a>

# NICE Challenge Labs

**Malicious Malware Option 2 | Cheryl Resch** 25h 48m Left [Submit Challenge Attempt](#)

Machine Name	Status	Actions	Open Console ?
ⓘ Having issues with mouse/keyboard input or connecting to VM consoles?			
Asteroids-PoS	Powered On	Action ▾	HTML5 VMRC
Asteroids-Router	Powered On	Action ▾	HTML5 VMRC
Centipede-PoS	Powered On	Action ▾	HTML5 VMRC
Centipede-Router	Powered On	Action ▾	HTML5 VMRC
Database	Powered On	Action ▾	HTML5 VMRC
Domain-Controller	Powered On	Action ▾	HTML5 VMRC
Fileshare	Powered On	Action ▾	HTML5 VMRC
Firewall	Powered On	Action ▾	HTML5 VMRC
Prod-Joomla	Powered On	Action ▾	HTML5 VMRC
Security-Desk	Powered On	Action ▾	HTML5 VMRC

Status	Check Description	Check Type	Check State	Last Changed
✓	Malicious Malware Removed	Challenge Check ?	Desired State	07:17 PM PDT
✓	Windows Malware Quarantined on Security-Desk	Challenge Check ?	Desired State	07:13 PM PDT

**Documentation** | Challenge Info | Meeting Notes | Network Map

Please enter any tools, programs, and utilities used to complete the challenge.

pscp.exe | Audit Process Tracking | Event Viewer | Local Security Policy |  +

Document all necessary steps and actions taken to complete the challenge in the field below. Document as if you were writing documentation for the company. This information will be sent to your challenge Curator for review.\*

(I followed the hints in order to identify the malicious file.)

The problem I encountered while trying to identify the malicious file was that it kept creating and terminating processes faster than I could visually identify. As such, I needed to have Windows track those processes into logs, for more detailed review.

# 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<sup>®</sup>**  
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

A satellite view of Earth from space, showing the Americas and the Atlantic Ocean. The image is tinted with a blue/cyan color. A bright starburst light is positioned in the center of the image, behind the text.

**Thank you!**