

# Mapping Low Cost and Open Source Labs to the NICE Workforce Framework and CAE KU's

Chris Simpson,  
Director National University Center for  
Cybersecurity

# Agenda

- Background
- Examples of free labs and how we use them
- Mapping labs to the NICE Framework and KU's

# Background

- Hands on labs are a critical component of any cybersecurity program and a requirement to become an NSA/DHS Center of Academic Excellence
- Several ways to deliver lab content
  - Develop and deploy labs on internal or outsourced infrastructure
  - Utilize labs from external lab providers
  - Utilize free grant resourced labs
  - Use free and open source labs
- Managing an internal lab environment is expensive

# Challenges of Running an Internal Lab

- Help Desk
  - Academic vs Technical issues
  - Hours of operation
    - Student complete school work in the evening and on weekends
  - “Ticket Management”
- Admin access to systems
- Developing lab content
- Cost

# Finding Outsourced Labs

- “Word of Mouth”
- Textbook Vendors
- Vendor booths
- Google

# Challenges of Free Labs

- Downtime
- Support
- Updates
- No single vendor provides everything you need
- Publicly available answers
- Course coverage of lab content
- Faculty preparation
- Vendor lab changes

# Free/Freemium Providers

- Not an official endorsement from National University

# Providers

(No particular order)

Immersive Labs  
(Free)

NICE Challenge  
(Free)

Over the Wire  
(Free)

PicoCTF (Free)

Hack The Box  
(Freemium)

TryHackMe.com  
(Freemium)

Blue Team Labs  
(Freemium)

# Immersive Labs Digital Cyber Academy

- Available to students, Veterans, and Neurodivergent community
- Question based, virtual machine based and scenario based labs

The screenshot shows the top navigation bar with links for 'MITRE ATT&CK', 'Leaderboard', 'Jobs', and 'More'. Below the navigation is a 'Browse' section with two featured labs. The first lab, 'Penetration Tester', features an illustration of a person in a red shirt and blue pants lying on a blue surface, surrounded by floating green and red cubes. The second lab, 'Become a Tier 1 SOC Analyst', features an illustration of a person in a blue shirt and red pants sitting at a desk with multiple computer monitors displaying code. The text for the 'Penetration Tester' lab reads: 'This objective will introduce you to the key knowledge areas required by Pen Testers. Pen Testers perform assessments of systems and identify where they deviate from acceptable configurations and...'. The text for the 'Become a Tier 1 SOC Analyst' lab reads: 'This objective will introduce you to the role of a Tier 1 SOC Analyst. SOC Analysts use data collection and analysis tools (e.g., IDS alerts, firewalls, SIEM logs, etc.) to detect and respond to security incidents...'. Both lab cards have a green checkmark in the bottom right corner.

# Immersive Labs

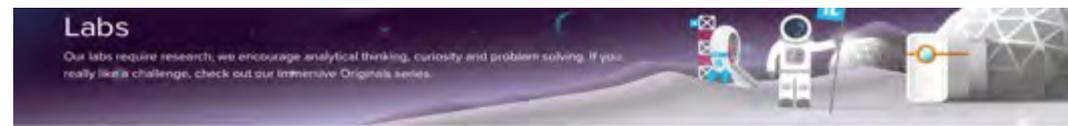
Badging

Large variety of topics

Novice to “Ninja”

Knowledge + Hands on

Rankings



Filter

Search

**Knowledge**  
Cover the basics! Master the fundamentals of cyber security with a series of introductory labs on cyber theory and industry scenarios.

Just Laid  
[What Is Risk?](#)

**Tools**  
From simple to advanced, this is where you will learn the nuts and bolts of the cyber security landscape. This includes how to use tools.

New Lab  
[Introduction to Command & Control Frameworks](#)

**Techniques**  
Time to flex those cyber skills! From ethical web hacking to malware analysis - Immersive Labs has you covered.

New Lab  
[Web Applications: Page Source Review](#)

**Immersive Originals**  
[Love a challenge? So do we! These are our Immersive Originals and all 5 you can't wait to take your best of friends.

New Lab  
[Immersive Labs and Your Employer](#)

**Secure Code**  
Learn the skills that test your ability to identify, exploit, secure and validate common vulnerabilities in code.

View 3 more

League Table Leaderboard

POSITION	AVATAR	USER	POINTS
1		Tech Vets	2883620
2		New York University	1692245
3		Edinburgh Napier University	1439130
4		National University Livi Politechnic	1270940
5		University of South Wales	1254385
6		DCA HSLU Lucerne University of Applied Sciences	1219620
7		Singapore Institute of Technology	1137050
8		Dakota State University	1079600
9		Nanyang Polytechnic	931885
10		Lancaster University	869940
11		Institute of Technical Education	812470
12		National University	735380



Desktop

Applications



Trash



File System



Home



LabFiles



Terminator



Ghidra



Chromium

Lab Progress

13%

### Tasks

1. Open the PCAP file located in the /labfiles/PCAPBasics/ directory.
2. Analyse the PCAP file, answer the questions and complete the lab.

Question 1 of 8

**What is the server name sought in the first DNS request that is issued by the client?**

Question 2 of 8

**What is the first IP address returned in the DNS response for the domain in Q1?**

Question 3 of 8

**What is the browser user agent string that issued the search request?**

The screenshot shows a user profile page for Chris Simpson. The user is at Level 37, with 151 points to reach the next level. They have earned 7,800 points and completed 44 labs. The page is divided into sections for Objectives and Labs. The Labs section is organized into two columns, each with a 'View Details' link.

Category	Progress	View Details
Self-Assigned	23%	<a href="#">View Details</a>
Fundamentals	3%	<a href="#">View Details</a>
Defensive	6%	<a href="#">View Details</a>
Cyber Threat Intelligence	0%	<a href="#">View Details</a>
Offensive	11%	<a href="#">View Details</a>
Tools	11%	<a href="#">View Details</a>
Malware & Reverse Engineering	0%	<a href="#">View Details</a>

# Reporting



# Over the Wire

- Community built labs
- Different games and levels
- Command line based
- Bandit great for learning Linux
- Under the Wire for PowerShell



## Wargames

The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games.

To find out more about a certain wargame, just visit its page linked from the menu on the left.

If you have a problem, a question or a suggestion, you can [join us via chat](#).

### Suggested order to play the games in

1. Bandit
2. Leviathan or Natas or Krypton
3. Narnia
4. Behemoth
5. Utumno
6. Maze
7. ...

### Each shell game has its own SSH port

Information about how to connect to each game using SSH, is provided in the top left corner of the page. Keep in mind that every game uses a different SSH port.



Bandit Demo

Bandit Demo

## Introducing the picoGym



picoGym is a noncompetitive practice space where you can explore and solve challenges from previously released picoCTF competitions, find fresh never before revealed challenges, and build a knowledge base of cyber security skills in a safe environment.

Whether you are a cyber security professional, competitive hacker or new to CTFs you will find interesting challenges in the picoGym that you can solve at your own pace. Team picoCTF will regularly update this challenge repository so visit the picoGym often.

[Practice picoGym](#)

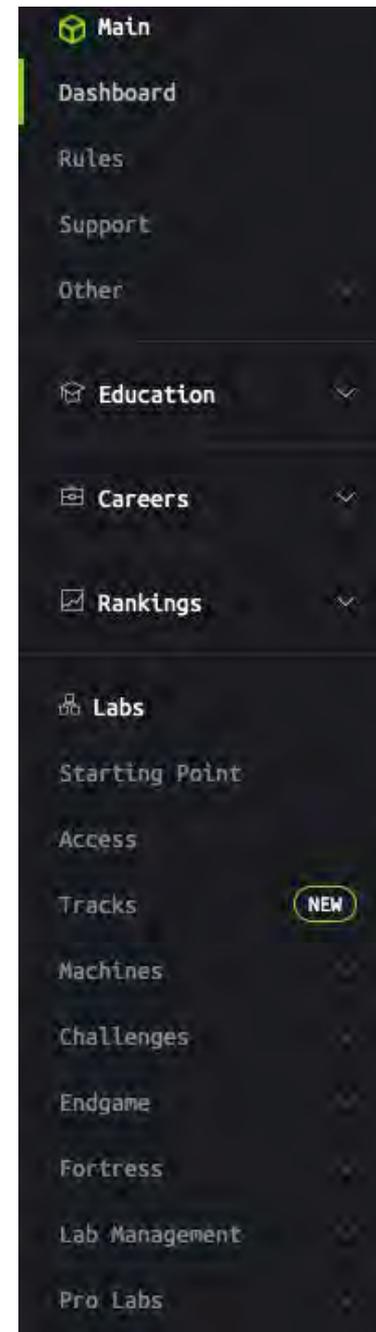
Challenge Name	Category	Points	Solves	Completion %
Lets Warm Up	General Skills	50	3,145	64%
The Numbers	Cryptography	50	2,116	52%
2Warr	General Skills	50	2,643	-
Insp3ct0r	Web Exploitation	50	2,089	73%
Glory of the Garden	Forensics	50	1,533	86%
vault-c	Reverse Engineering	50	1,420	-
Warmed Up	General Skills	50	-	-
vault-door-1	Reverse Engineering	100	-	-
what's	General Skills	50	-	-

# PicoCTF

- Designed by Carnegie Mellon
- Designed for high school students
- Great for anyone new to cybersecurity

# Hack the Box

- Freemium model
- Vulnerable hosts
  - Active
  - Retired
- Challenges
- Scenarios
- "Hack" into hosts
- Linux and Windows
- Difficulty ratings
- Ranking system
- Active and Retired Machines
- Can share answers for retired machines
- Set of challenges
- Beginner to expert







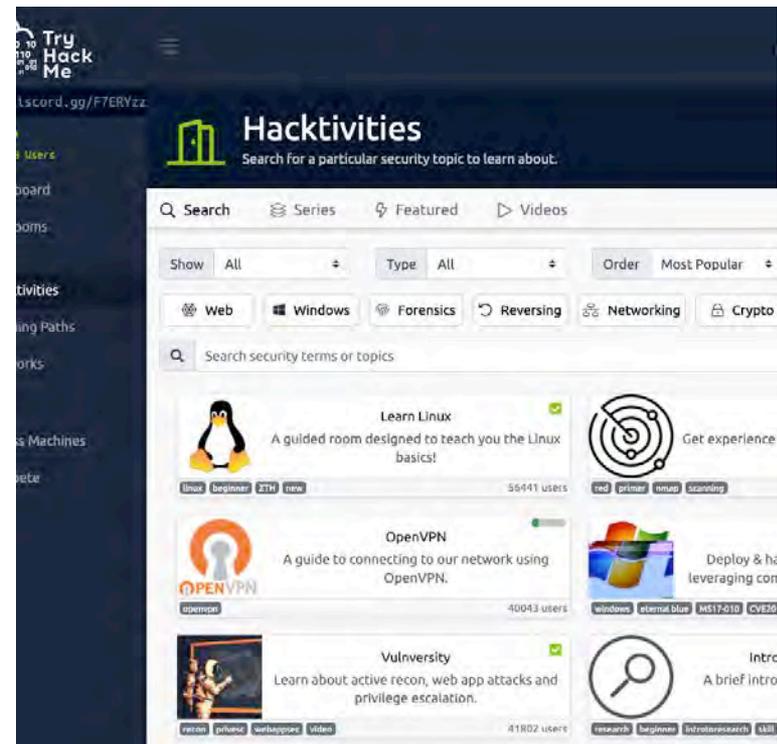
# Videos and Tutorials

- Twitch.TV
  - [https://www.twitch.tv/r00k\\_infosec/](https://www.twitch.tv/r00k_infosec/)
- YouTube - Ippsec
- <https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA>



# TryHackMe

- Community Built
- Variety of topics
- Room Concept
- East to build your own VM and upload
- Clone and customize rooms



# TryHackMe

**Task 1** Recon ☰ ▼

Scan and learn what exploit this machine is vulnerable to. Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up. This room is not meant to be a boot2root CTF, rather, this is an educational series for complete beginners. Professionals will likely get very little out of this room beyond basic practice as the process here is meant to be beginner-focused. Deploy



Art by one of our members, Varg - THM Profile - Instagram - Blue Merch

**#1** Scan the machine. (If you are unsure how to tackle this, I recommend checking out the room [RP: Nmap](#))

Completed Hint

**#2** How many ports are open with a port number under 1000?

Submit Hint

**#3** What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

Submit Hint

**Task 2** Gain Access ▼

**Task 3** Escalate ▼

**Task 4** Cracking ▼

**Task 5** Find flags! ▼



# Hacktivities

The learning path to learn about

378

Public Rooms

- Overview
- All Rooms
- Settings

## Learning Paths

Work your way through a structured learning path

**CYBER DEFENSE**

Learn how to analyse and defend against real world cyber threat scenarios

- Detect threats
- Gather threat actor intelligence
- Understand and simulate adversary TTPs
- Identify and respond to incidents

12 lessons 12 lessons

**COMPLETE BOSSWICH**

Learn the core skills needed to start a career in cyber security

- Web app browser security
- Network security
- Basic Linux
- Scripting

10 lessons 10 lessons

**OFFENSIVE PENTESTING**

Prepare yourself for real world penetration testing

- Utilise industry standard tools
- Learn realistic attack scenarios
- Plan an offensive security
- Supporting exercises & resources

10 lessons 10 lessons

# Pre Security

## Hacktivities

Find a security topic to learn about.

441  
Public Rooms

Overview

All Rooms

Series

63 new Rooms

## Learning Paths

Work your way through a structured learning path



**PRE SECURITY**

Before hacking something, you first need to understand the basics.

- Cyber security basics
- Networking basics and weaknesses
- The web and common attacks
- Learn to use the Linux operating system

🕒 40 Hours

🏠 16 Rooms



**CYBER DEFENSE**

Learn how to analyse and defend against real-world cyber threats/attacks

- Detect threats
- Gather threat actor intelligence
- Understand and emulate adversary TTPs
- Identify and respond to incidents

🕒 48 Hours

🏠 39 Rooms



**COMPLETE BEGINNER**

Learn the core skills required to start a career in cyber security

- Web application security
- Network security
- Basic Linux
- Scripting

🕒 64 Hours

🏠 33 Rooms

# Blue Team Labs (Hack the Box for Blue Teams)

- Community Built
- Variety of topics
- Room Concept
- Ranks and badges
- Deploys VM's

The screenshot displays the Blue Team Labs Online dashboard. At the top, the logo and name 'Blue Team Labs Online' are visible, along with a button to 'Register your interest in Op Chimera for free!'. The navigation bar includes links for Home, Investigations (with PRO and FREE tags), Challenges (with FREE tag), Leaderboard, Manage subscription, Collectibles, and Feedback. The main content area features four statistics cards: Investigations Completed / Total (2 / 58), Challenges Completed / Total (5 / 26), Your Points / Total Points (207 / 3085), and Top 3% of Defenders (# 320 / 12319). Below these is a welcome message and a list of action buttons: View Investigations, View Challenges, View Your Profile, Highlight Badges & Titles, Redeem Code, and Help / FAQ.

Blue Team Labs Online

Register your interest in Op Chimera for free!

Home Investigations PRO FREE Challenges FREE Leaderboard Manage subscription Collectibles Feedback

2 / 58 Investigations Completed / Total

5 / 26 Challenges Completed / Total

207 / 3085 Your Points / Total Points

# 320 / 12319 Top 3% of Defenders

Welcome to Blue Team Labs Online !

Please familiarise yourself with our Platform Rules. This will ensure you're aware of our restrictions regarding publishing writeups, sharing answers, and other activities.

Our platform is the perfect place for established cyber defenders to practice in realistic scenarios and showcase their skills in a gamified and competitive environment. Paired with external training or self-study BTLO can develop your technical capability to investigate and defend against cyber attacks and intrusions.

Good luck Defenders!

View Investigations

View Challenges

View Your Profile

Highlight Badges & Titles

Redeem Code

Help / FAQ ?

# Blue Team Labs

The screenshot displays the Blue Team Labs Online web application. At the top, there is a navigation bar with icons for Home, Investigations (PRO), Challenges (FREE), Leaderboard, Manage subscription, Collectibles, and Feedback. A blue banner at the top right encourages users to register for Op Chimera. The main content area features a challenge titled "SAM" with a difficulty of "Medium" and 50 points. The challenge description states: "Samuel (Sam) is a Neatnik, when it comes to cleanliness and hygiene. Find out if he also follows cyber hygiene. An incident has been reported stating 'Sam has lost his SAM'. It's your job to figure out what has happened. You are provided with sysmon logs, network traffic, and a memory dump." The challenge is categorized under "Linux CLI", "Wireshark", and "Volatility2". Below the description, there is a "Start Investigation" button and a table showing the challenge's statistics: 50 points, Medium difficulty, 91 solves, and Linux OS. The challenge is created by "First-Blood". The right-hand side of the interface shows the "Scenario" section, which repeats the challenge description. Below this is the "Investigation Submission" section, which contains three questions with their respective point values and submission buttons: "What is the attacker IP, and what is the port that they got a reverse shell on? (3 points)", "What's the name of the malicious file that gave remote access to attacker? (4 points)", and "What is the process that has been called by the payload upon execution? (5 points)".

Blue Team Labs Online

Register your interest in Op Chimera for free!

Home Investigations PRO FREE Challenges FREE Leaderboard Manage subscription Collectibles Feedback

## SAM

Samuel (Sam) is a Neatnik, when it comes to cleanliness and hygiene. Find out if he also follows cyber hygiene. An incident has been reported stating "Sam has lost his SAM". It's your job to figure out what has happened. You are provided with sysmon logs, network traffic, and a memory dump.

Linux CLI Wireshark Volatility2

Start Investigation

Points	Difficulty	Solves	OS
50	Medium	91	Linux

First-Blood Created By

### Scenario

Samuel (Sam) is a Neatnik, when it comes to cleanliness and hygiene. Find out if he also follows cyber hygiene. An incident has been reported stating "Sam has lost his SAM". It's your job to figure out what has happened. You are provided with sysmon logs, network traffic, and a memory dump.

### Investigation Submission

What is the attacker IP, and what is the port that they got a reverse shell on? (3 points)

Format: IP, port

Submit

What's the name of the malicious file that gave remote access to attacker? (4 points)

Format: filename.extension

Submit

What is the process that has been called by the payload upon execution? (5 points)

Format: processname.extension

Submit

Knowing the payload name and process name, if the payload was generated by msfvenom, what would be the format option that the attacker would've used? (5 points)

msfvenom Payload Type

Submit



# Deploy in the Cloud

- Use Devops tools to deploy labs in the cloud
- Examples
  - Detection Lab
  - Mordor
  - CyberRange

# Nice Challenge

Excellent set of challenges

Mapped to NICE  
Framework

Free

Reservations required

# Mapping Labs To Objectives

Build a catalog of  
labs mapped to the  
NICE Framework  
and CAE KU's

Student project  
mapping  
TryHackMe

Using AirTable

# Some challenges to mapping labs

Too many labs

Too many  
KSAT's

KU topic vs  
outcomes

KU not as easy  
to import

# What is AirTable

CLOUD BASED  
SPREADSHEET/DATABASE

A BASE IS A SET OF  
TABLES

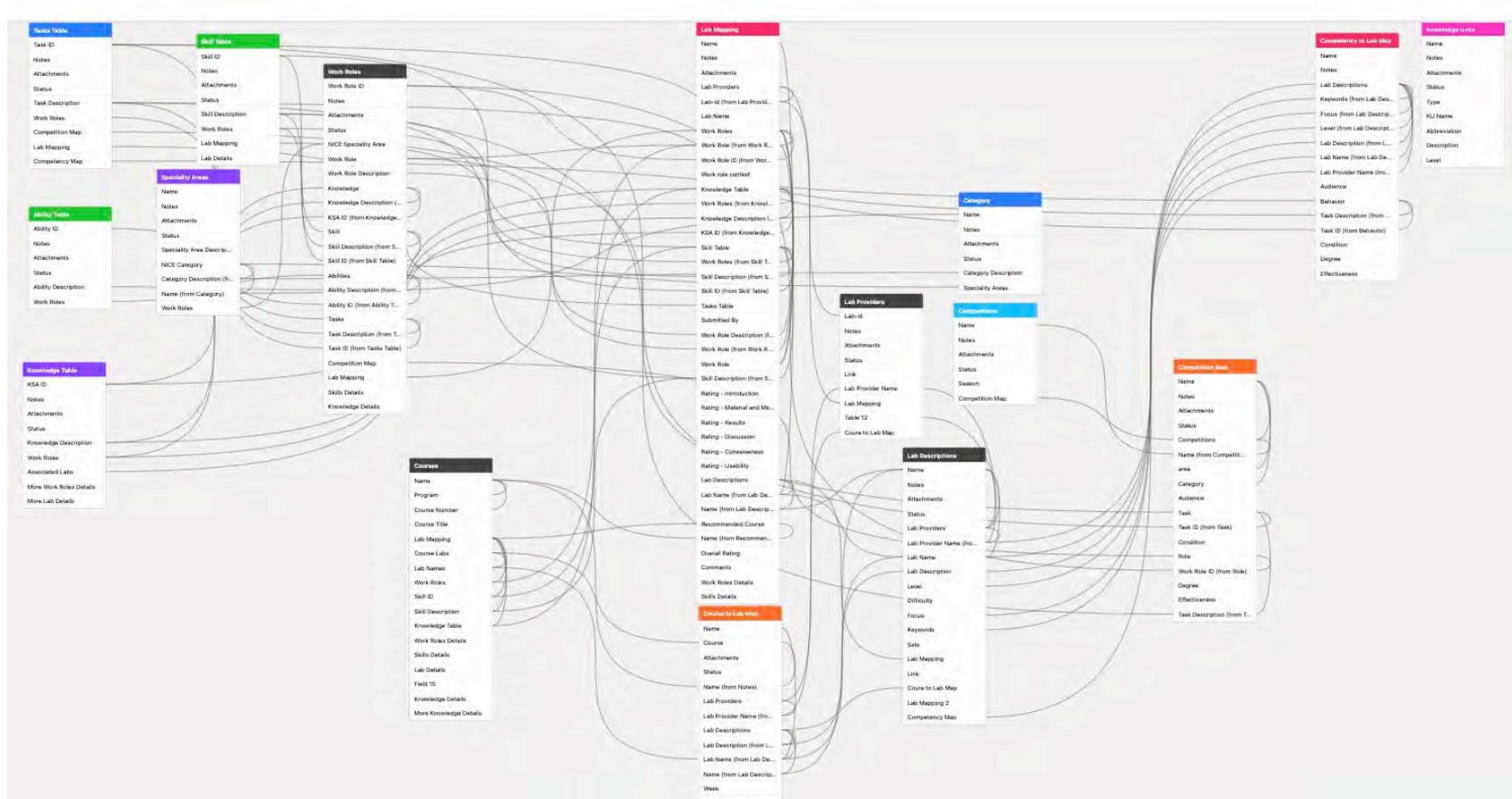
TABLES USE ROWS AND  
COLUMNS

EASY TO CONNECT  
TABLES

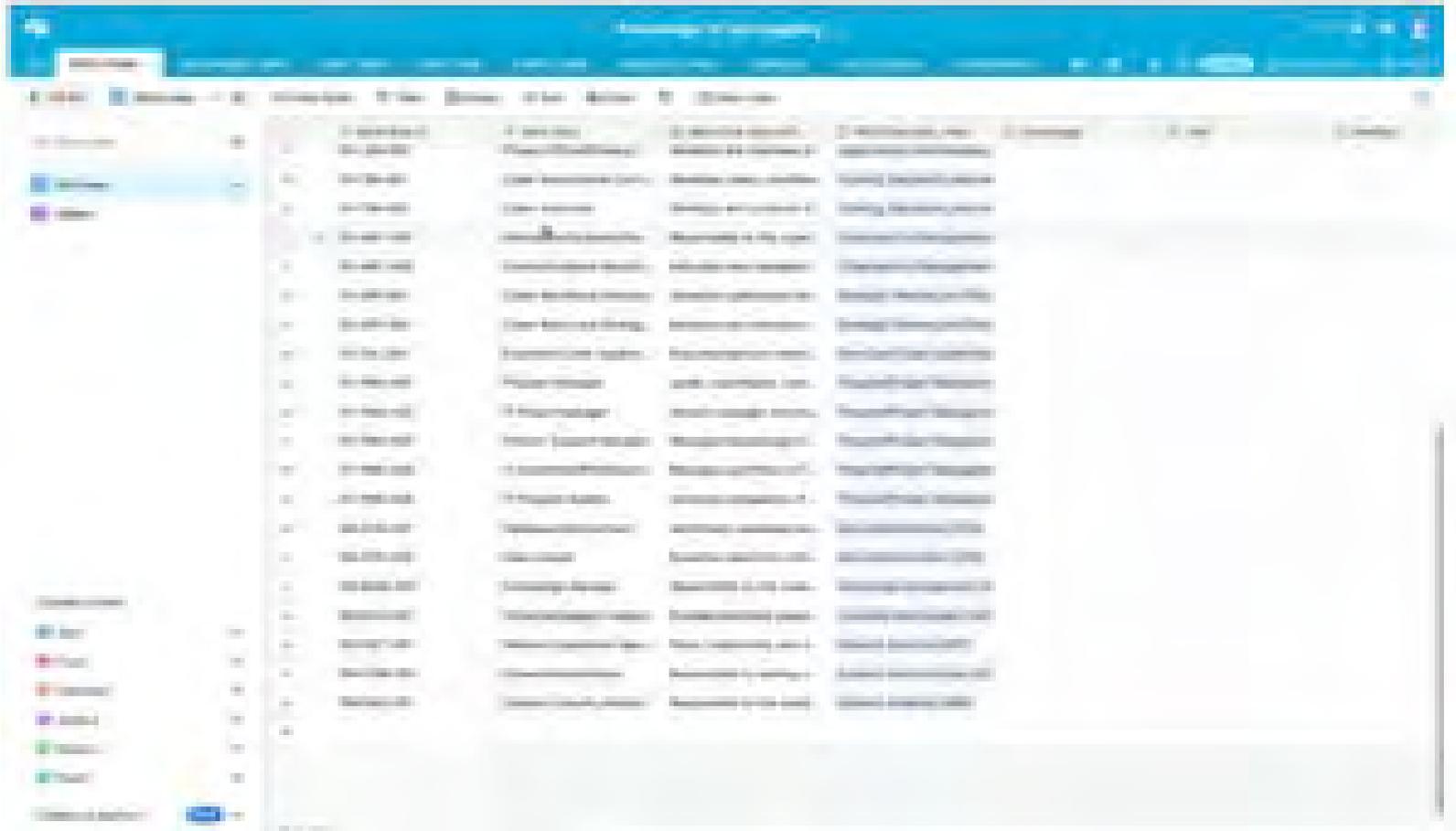
DOESN'T REQUIRE  
DETAILED DATABASE  
PLANNING

CAPABILITY TO CREATE  
FORMS

# Database Design



# Airtable Demo





CLARK

# Clark Center

- Digital repository for cybersecurity curriculum
- Built to store content
- Supports Bloom's Taxonomy
- Easy search for KSATs and KU's plus other frameworks
- Crowdsourced mapping
- Not for external labs
- <https://clark.center/>

# Clark Center Example

← Back



SUBMIT FOR REVIEW →

Basic Information

Learning Outcomes

Materials

All changes saved

Children

Add Child +

This learning object has no children

## 2 Learning Outcomes

Discover open ports on a network using Nmap.



Remember & Understand



Apply & Analyze



Evaluate & Synthesize

Discover ▾ open ports on a network using Nmap.

Maps to:

NICE Cybersecurity Workforce Framework Tasks - T0028 - 2017 ×

CAE Cyber Defense - Basic Networking (KUS) - 2019 ×

CAE Cyber Defense - Network Defense - 2014 ×

NICE - S0081 - 2020 ×

NICE - T0549 - 2020 ×

NICE - T0010 - 2020 ×

NICE - T0188 - 2020 ×

## Curricular Guidelines

Search curricular guidelines...



7 suggestions

CAE Cyber Defense - Network Defense - 2014

Students will be able to use a network mapping tool (e.g., Nmap).

NICE - S0081 - 2020

Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).

Cyber2yr2020 - Cross-Cutting Concepts [CC-5] - 2020

Discuss how changes in one part of a system may impact other parts of a cybersecurity ecosystem.

# Centers of Academic Excellence in Cybersecurity Resource Directory (CARD)

- Categorized collection of cybersecurity education resources developed by members of the cybersecurity community
- No KU/KSAT mapping



<https://www.caeresource.directory/>

# Some Other Takeaways

- Students can share achievements
- Capstone projects
- Invitation to attend capstone
  - TryHackMe Throwback
  - Hack the Box Dante

Truly enjoyed the Throwback Network from TryHackMe! Awesome setup for learning network pentesting and attacking Windows Active Directory. Thank you [TryHackMe!](#)

[#tryhackme](#) [#throwback](#) [#thm](#) [#activedirectory](#) [#pentesting](#)



# Cyber Competition Coach and Mentor Training

Home

SoCal Cyber Cup Mentor Training Edit

- Announcements
- Modules
- Syllabus
- People
- Assignments
- Discussions
- Quizzes
- Grades
- Pages
- Files
- Outcomes
- Conferences
- Collaborations
- Rubrics
- New Analytics
- Settings



Welcome Everyone to the SoCal Cyber Cup Mentor Training. This training course includes a set of 20 different modules to help you learn and understand what it takes to become an Outstanding Mentor. There are four different types of modules that you will be experiencing and each provides you with different tools that you need to provide the leadership and mentorship for your Cybersecurity student teams. The modules are grouped by area including Mechanics (background needed to understand the competitions), Team/Collaboration/Ethics, Topical/Technical Training, and free resources. It is our intent to provide you with tools that you and your team can use in preparation for the competition. Since we all come in with a variety of skill sets, you do not need to feel obligated to go through every module or even in the order that they are listed but use these modules as you have questions or need information to help you and your teams be successful. Have Fun, Good Luck, and remember YOU ARE NOT IN

- Import Existing Content
- Import from Commons
- Choose Home Page
- View Course Stream
- New Announcement
- New Analytics
- View Course Calendar
- View Course Notifications

To Do

Nothing for now

Recent Feedback

Nothing for now



Questions?

Email: [csimpson@nu.edu](mailto:csimpson@nu.edu)

# Links

- <https://www.immersivelabs.com/digital-cyber-academies/>
- <https://overthewire.org/wargames/>
- <https://underthewire.tech/>
- <https://www.hackthebox.eu/>
- <https://www.picoctf.org/>
- <https://tryhackme.com/>
- <https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA>
- [https://www.twitch.tv/r00k\\_infosec/](https://www.twitch.tv/r00k_infosec/)
- <https://www.detectionlab.network/>
- <https://mordordatasets.com/introduction.html>
- <https://medium.com/aws-cyber-range>
- <https://clark.center/home>
- <https://github.com/carnal0wnage/weirdAAL>
- <https://github.com/RhinoSecurityLabs/cloudgoat>
- <https://rhinosecuritylabs.com/aws/assume-worst-aws-assume-role-enumeration/>
- <https://airtable.com/>