

# Use of Free and Open Source Labs to Support Cybersecurity Education (Fall 2019 Edition)

Chris Simpson,  
Director National University Center  
for Cybersecurity



# Agenda

- Purpose
- National University's journey to outsourced labs
- Challenges of using outsourced labs
- Lab Demo
- KU Mapping



# Background

- Hands on labs are a critical component of any cybersecurity program and a CAE requirement
- 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



# Background

- Many externally provided labs aren't mapped to CAE Knowledge Units or the NICE Framework, especially the open source labs.
- This makes it challenging for schools to identify the right labs for their program and requires extensive efforts to map the labs to meet these different requirements.
- There is duplicated effort as different institutions map the same labs and in many cases will map them to the same knowledge units and NICE KSA's.



# National University's Lab Journey

- MS Cybersecurity Program started 2011
- Created Virtual Lab Environment (VEL)
  - Outside contractor
  - Surplus hardware
  - VMWARE environment
- Migration to lab managed by IT Department
  - Information Security Lab Environment



# 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



# Picking the right labs

- Most vendors don't map to KU/KSA's
- Some selection criteria
  - Quality of labs
  - Ease of access (LMS integration)
  - Cost
  - Security
- Lab Types
  - Directive vs Non Directive
  - Scenario vs Non Scenario





# Providers

- Not an official endorsement from National University



# Providers

(No particular order)

## Current

- Circadence (Paid)
- Immersive Labs (Free)
- Infosec Learning (Paid)
- ITPro.tv (Paid)
- National Cyber League
- NICE Challenge (Free)
- Over the Wire (Free)
- PicoCTF (Free)
- Hack The Box (Freemium)

## Researching

- Linux Academy (Paid)
- AttackDefense.com (Paid)
- Deploy your own in the cloud with Devops tools



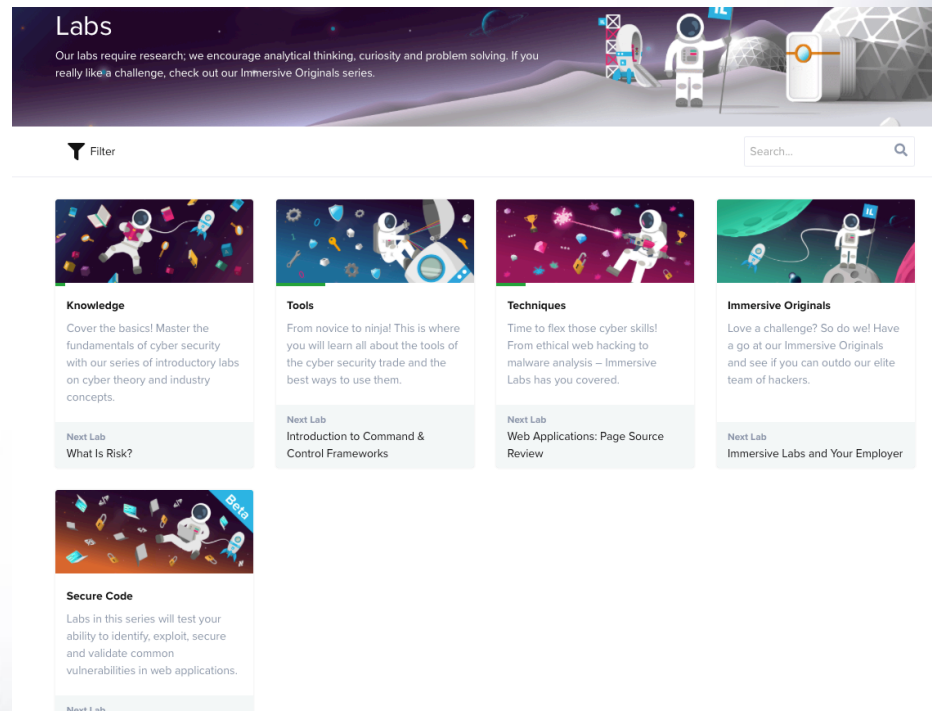
# Challenges of Outsourced Labs

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



# Immersive Labs

- Badging
- Large variety of topics
- Novice to “Ninja”
- Knowledge + Hands on
- Rankings

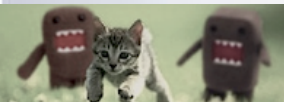


The screenshot displays the 'Labs' section of a website. At the top, there is a header with the word 'Labs' and a sub-header: 'Our labs require research; we encourage analytical thinking, curiosity and problem solving. If you really like a challenge, check out our Immersive Originals series.' Below the header is a navigation bar with a 'Filter' button and a search box containing the text 'Search...'. The main content area features a grid of lab cards. Each card has a colorful illustration at the top, a title, a brief description, and a 'Next Lab' link.

Lab Title	Description	Next Lab
<b>Knowledge</b>	Cover the basics! Master the fundamentals of cyber security with our series of introductory labs on cyber theory and industry concepts.	What Is Risk?
<b>Tools</b>	From novice to ninja! This is where you will learn all about the tools of the cyber security trade and the best ways to use them.	Introduction to Command & Control Frameworks
<b>Techniques</b>	Time to flex those cyber skills! From ethical web hacking to malware analysis – Immersive Labs has you covered.	Web Applications: Page Source Review
<b>Immersive Originals</b>	Love a challenge? So do we! Have a go at our Immersive Originals and see if you can outdo our elite team of hackers.	Immersive Labs and Your Employer
<b>Secure Code</b>	Labs in this series will test your ability to identify, exploit, secure and validate common vulnerabilities in web applications.	

# Over The Wire

- Command line based
- Need access to a terminal
- Hands on, solve and move to the next level,
- Areas
  - Basic Linux – Bandit
  - Web Security – Natas
  - Programming bugs – Vortex
- Beginner to expert



# Hack the Box

- "Hack" into hosts
- Linux and Windows
- Difficulty ratings
- Ranking system
- Active and Retired Machines
- Set of challenges
- Beginner to expert



# Pico CTF

- High school competition
- Great for students new to cybersecurity
- Q&A style
- Beginner to intermediate



# Deploy in the Cloud

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





# 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>



# Demo Time

- Immersive Labs
- Over the Wire
- Hack the Box
- PicoCTF
- Deploy in the Cloud



# Questions?

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



# KU Mapping



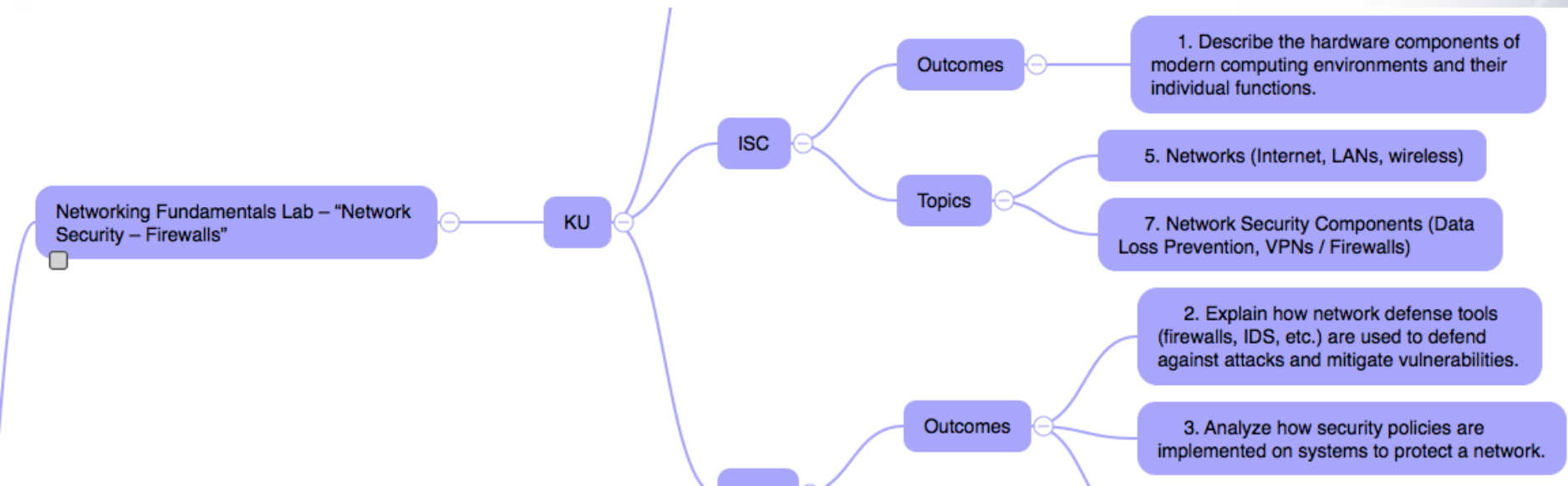
# Goal

- Build a framework and tool to easily map labs to CAE Knowledge Units and NICE KSA's and:
  - Allows for easy reporting of requirements
  - Allows for easy discovery of relevant labs for schools in search of labs



# How we mapped labs to KU/KSA's

- Manually reviewed lab content
- Mapped to knowledge unit
- Used CyberEd wiki to crosswalk to KSA
- Subjective



# KU → NICE Crosswalk

## Network Defense (2020)

The intent of the **Network Defense Knowledge Unit** is to provide a set of knowledge and skills that can be taken to protect a network and communicate with it.

### Contents [hide]

- 1 Outcomes
- 2 Topics
- 3 Skills
- 4 NICE Framework Categories
- 5 Specialization Areas
- 6 See also
- 7 Further reading
  - 7.1 Suggested textbooks
  - 7.2 Suggested academic readings
- 8 Sample knowledge test
- 9 Sample skills test
- 10 Sample abilities test
- 11 Additional notes or materials
- 12 Contacts
- 13 Reference ID

## NIST Special Publication 800-181

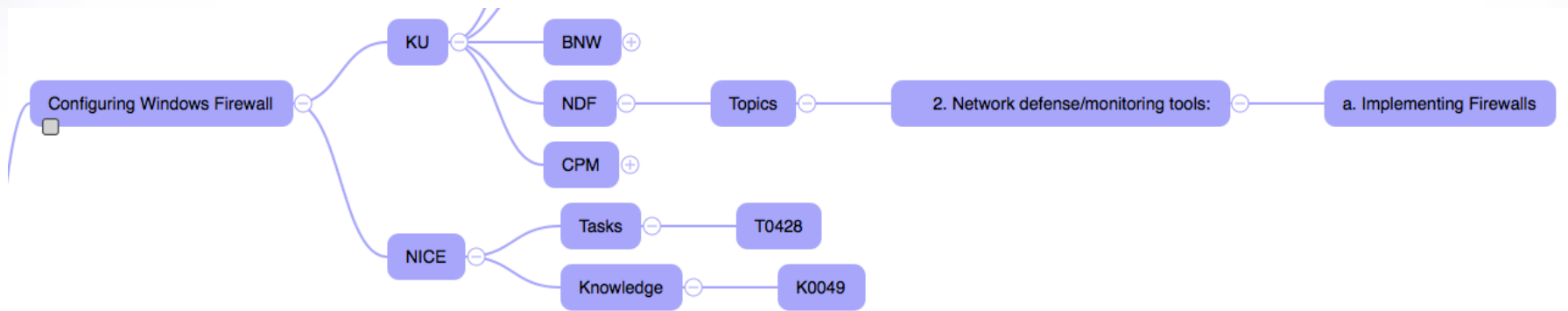
# National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

## NICE Framework Categories [edit]

- Securely Provision (SP)
- Operate and Maintain (OM)
- Analyze (AN)
- Collect and Operate (CO)

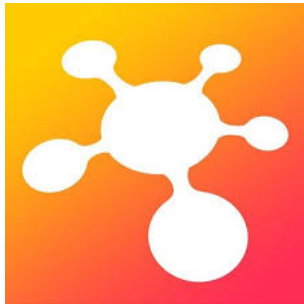


# KU → NICE Crosswalk





# Collecting and storing mappings



iThoughts



1. Export from mind map to csv file
2. Import to Excel
3. Clean up columns

# Example

Course	Lab Provider	Lab Name	Frame work	Code	Type or ID#	Description	Sub Topic
CYB 212	IL	Networking Fundamentals Lab: The OSI Model	KU	BNW	Topics	1. Networking models (OSI and IP).	
CYB 212	IL	Networking Fundamentals Lab: The OSI Model	KU	BNW	Topics	5. Network Protocols introduction (IP, TCP, UDP, ICMP)	
CYB 212	IL	Networking Fundamentals Lab: The OSI Model	KU	NTP	Outcomes	1. Network Switching (Ethernet)	a. ARP and RARP

Course	Lab Provider	Lab Name	Frame work	Code	Type or ID#
CYB 213	J&B	Configuring Windows Firewall	NICE	Tasks	T0428
CYB 213	J&B	Configuring Windows Firewall	NICE	Knowledge	K0049



# How to manage and share information?

- Build web based database with lab and mappings
- How to get there?
- Initial ideas
  - Spreadsheet/CSV
  - Mind Maps
  - Share via github



# Where to find mappings

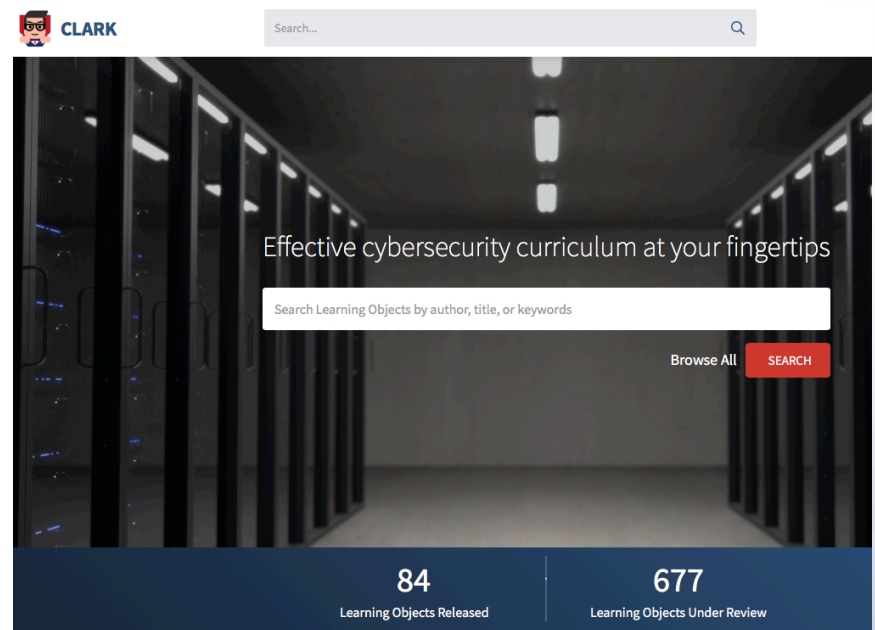
- <https://github.com/NU-Cybersecurity/labmapping>
  - Spreadsheets and mind maps



# New Discovery



<http://nccp.clark.center>



<http://clark.center>





## Description

The NICE Challenges are hands-on scenarios designed to bring the workforce experience to students before they enter the workforce and are free to U.S. based educational institutions.

Each challenge starts with a scenario written in the form of a task to complete from a fictional superior. For this module, it is as follows...

"Our CEO hired a contractor to audit our infrastructure. The auditor discovered our webserver is vulnerable to a recently discovered exploit. Create and apply an IDS/IPS ruleset that will prevent malicious requests of this nature from reaching the web server, while leaving benign traffic uninterrupted."

**Lab Environment:** The NICE Challenge Webportal is the lab environment used to complete and review NICE Challenges. The Webportal is a web platform which allows its users to interact with virtual environments and complete challenges requiring only a web browser. Details on how to sign-up as an educator and get started are in the notes section.

## Academic Levels

Undergraduate

Graduate

Post Graduate

Community College

## Learning Outcomes

Test that benign web traffic is not being prevented from reaching the web server.

(1 Mapped Outcomes)

Apply the new Snort ruleset on the core firewall to prevent malicious requests from reaching the web server.

(1 Mapped Outcomes)

Create a new Snort ruleset on the core firewall to prevent malicious requests from reaching the web server.

(16 Mapped Outcomes)

# Way Ahead

- Leverage tools like Clark and Github to crowdsource lab information
- Leverage CAE buying power



# Links

- [https://github.com/secdevops-cuse/CyberRange/blob/master/tutorials/getting\\_started.md](https://github.com/secdevops-cuse/CyberRange/blob/master/tutorials/getting_started.md)
- <https://github.com/hunters-forge/mordor>
- <https://mordor.readthedocs.io/en/latest/index.html>
- <https://medium.com/@clong/introducing-detection-lab-61db34bed6ae>
- <https://www.hackthebox.eu/>
- <https://picoctf.com>
- <https://www.hackthebox.eu/>
- <http://overthewire.org/wargames/>
- <https://immersivelabs.online/>

