Mapping Outsourced Labs to CAE KU's and NICE KSA's

Chris Simpson,

Director National University Center for Cybersecurity

Agenda

- Purpose

- Background

- National University's journey to outsourced labs

- Challenges of using outsourced labs

- Building a method to share lab information

About National University

- Among the largest private, nonprofit universities in California, dedicated to serving a diverse student population such as working parents, educators and members of our armed forces.

- Accelerated format
  - One month class
  - Students take one class at a time
  - Each class is 4.5 quarter hours
    - Same amount of material as in a regular quarter length course
  - Online/Onsite/Hybrid
  - Onsite meets twice a a week 5:30pm-10pm plus one Saturday
  - Cohort model

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

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

Current

- Circadence (Paid)
- Immersive Labs (Free)
- ITPro.tv (Paid)
- Jones & Bartlett (Paid)
- NICE Challenge (Free)
- Over the Wire (Free)
- PicoCTF (Free)

Researching

- Hack The Box (Freemium)
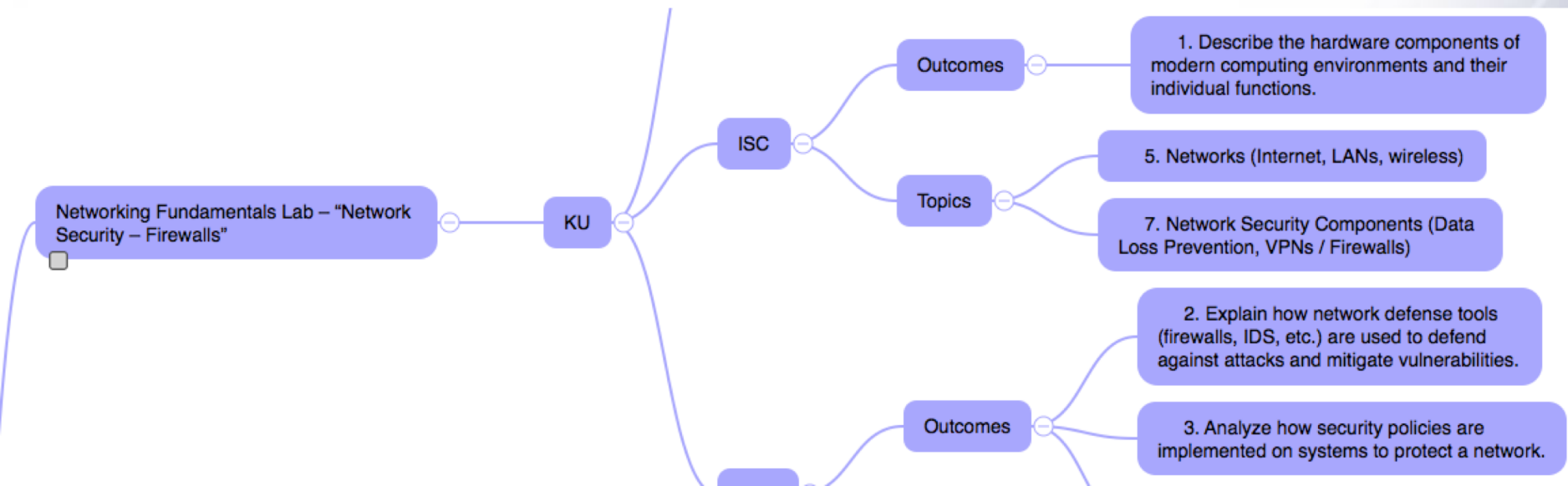- Linux Academy (Paid)
- AttackDefense.com (Paid)

Challenges of Outsourced Labs

- Downtime

- Support

- Updates

- Cost

- No single vendor provides everything you need

- Publicly available answers

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
that can be taken to protect a network and communic

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
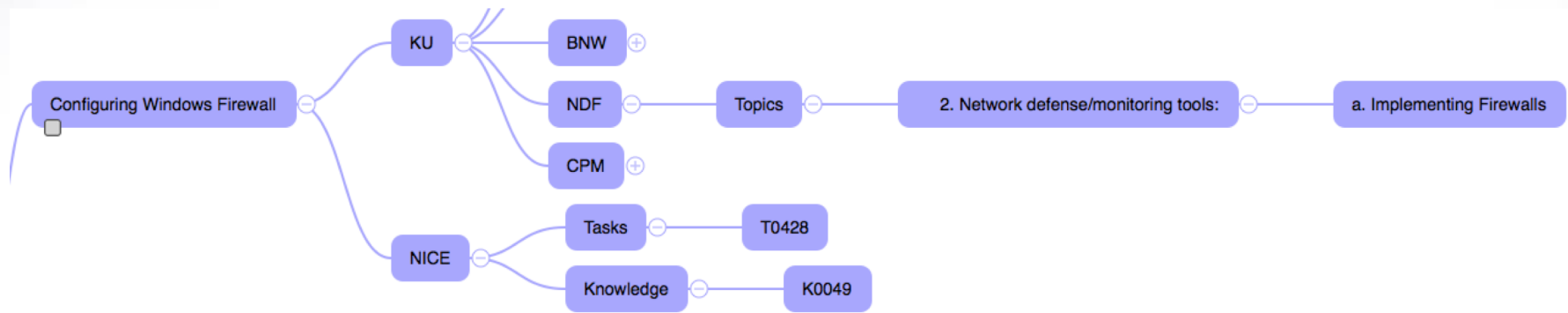12 Contacts
13 Reference ID

NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

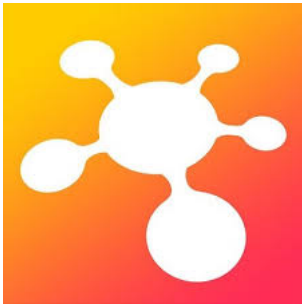## NICE Framework Categories [edit]

- 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
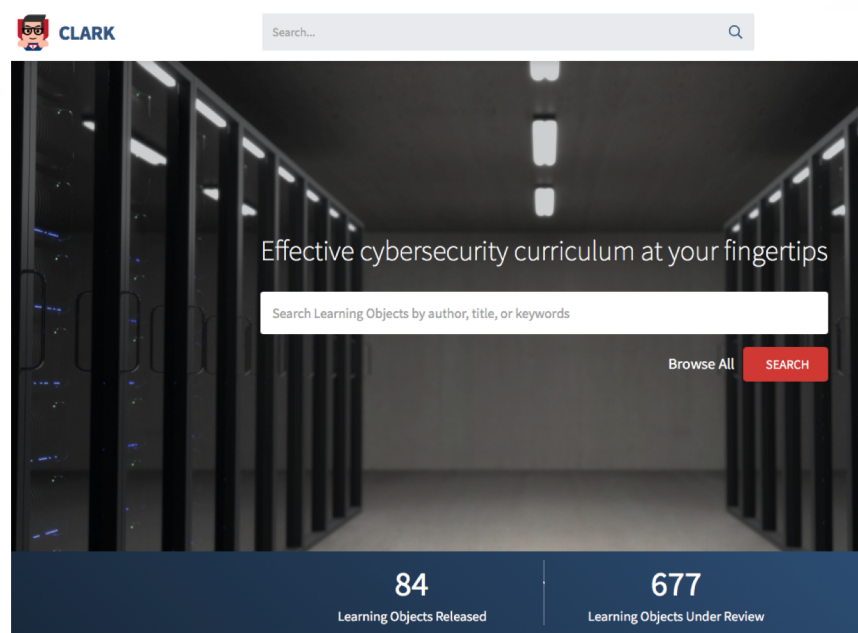
Description

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

Questions?

Email: csimpson@nu.edu