A Holistic Approach to Conducting a Cybersecurity Capstone Course

Vincent Nestler Ph. D.

Professor, California State University, San Bernardino

Principal Investigator, NICE Challenge Project

Lead, CAE Competency Working Group

Holistic approach

- Holistic
  - Characterized by the treatment of the whole person
  - Characterized by the belief that the parts of something are interconnected and can be explained only by reference to the whole.
- Capstone
  - Culminating experience, comprehensive
  - Last chance to catch, correct, prepare students for the workforce.
- Purpose
  - Explore what they think they want to do
  - Competent upon graduation at doing it
  - Be able to successfully interview for it

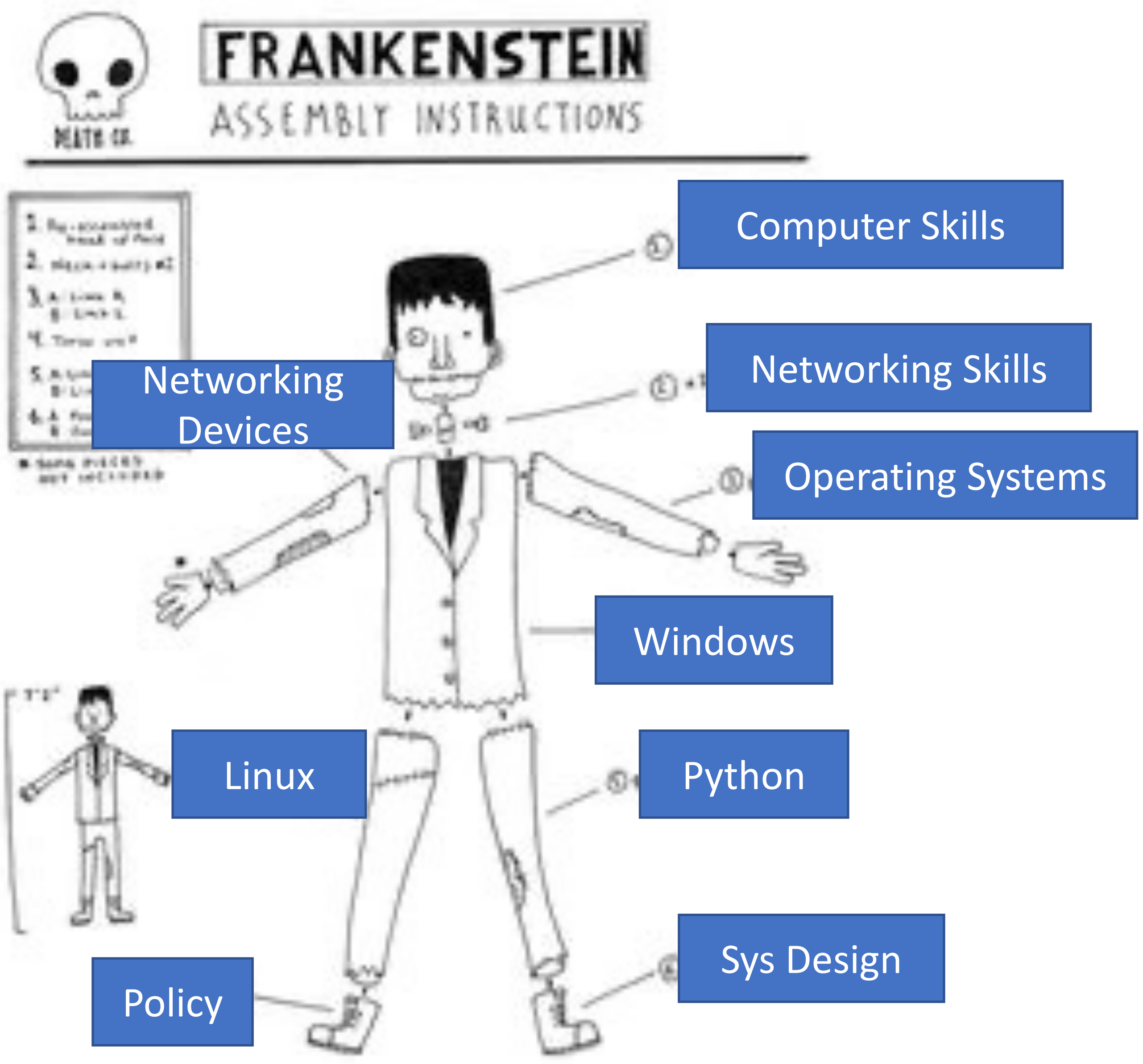
The Disconnect Between the Workforce and Academia

- What the workforce needs
- How academics interpret those needs
- How academia delivers
- Outcomes

Educating Frankenstein

Educating Frankenstein

- Computer Skills
- Networking Skills
- Operating Systems
- Network Devices
- Windows
- Linux
- Coding and Scripting
- etc



Computer Skills

Networking Skills

Networking Devices

Operating Systems

Windows

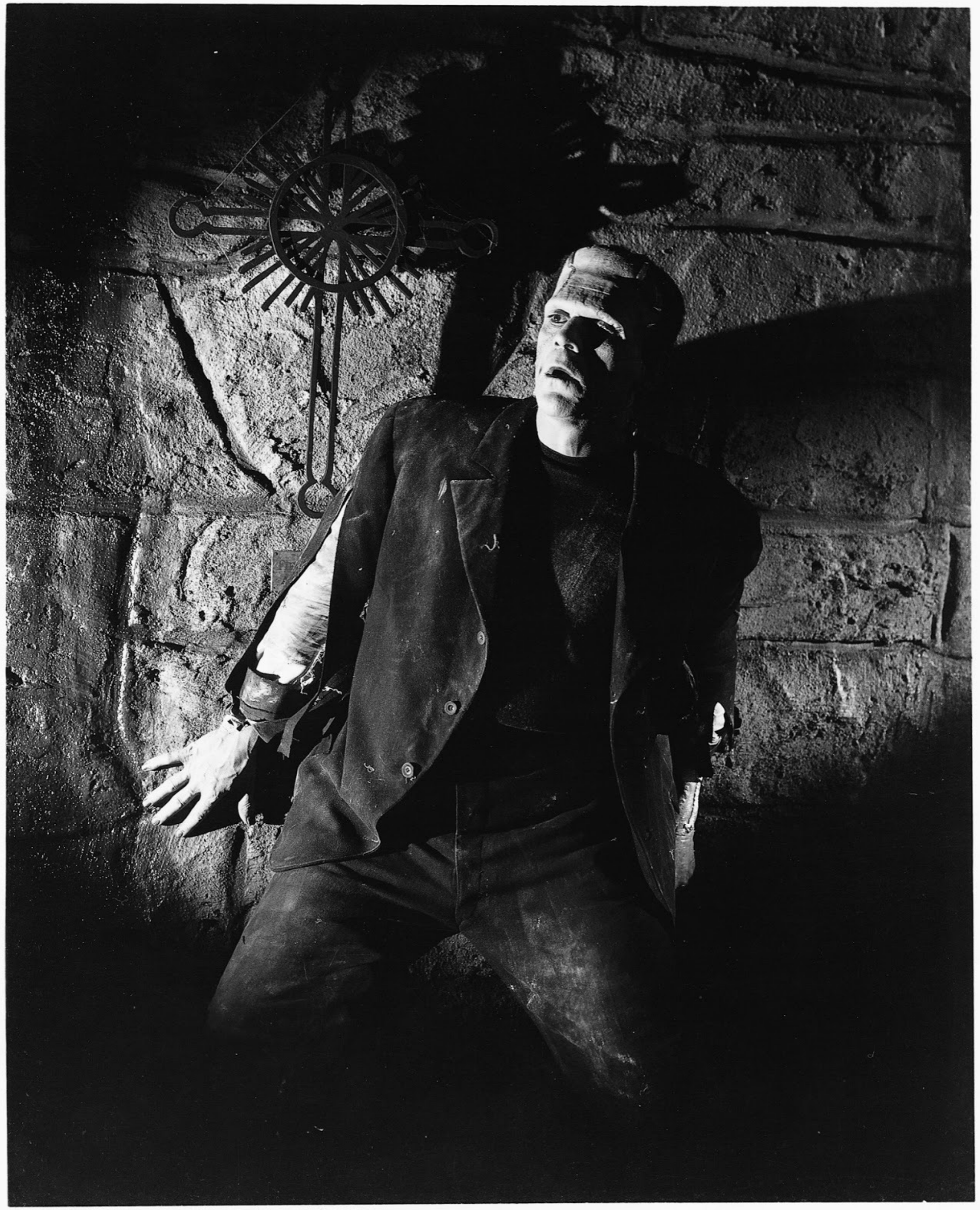
Linux

Python

Policy

Sys Design

CRACKER
INTRUDER
SPYWARE
PASSWORD
IDENTITY
UNSAFE
CODE
THEFT
HACKER
23487923
91236 142323
5678234
8765432



52 Work Roles

Authorizing Official/Designating Representative

Security Control Assessor

Software Developer

Secure Software Assessor

Enterprise Architect

Security Architect

Research & Development Specialist

Systems Requirements Planner

System Testing and Evaluation Specialist

Information Systems Security Developer

Systems Developer

Database Administrator

Data Analyst

Knowledge Manager

Technical Support Specialist

Network Operations Specialist

System Administrator

Cyber Policy and Strategy Planner

Executive Cyber Leadership

Program Manager

IT Project Manager

Product Support Manager

IT Investment/Portfolio Manager

IT Program Auditor

Cyber Defense Analyst

Systems Security Analyst

Cyber Legal Advisor

Privacy Officer/Privacy Compliance Manager

Cyber Instructional Curriculum Developer

Cyber Instructor

Information Systems Security Manager

Communications Security (COMSEC) Manager

Cyber Workforce Developer and Manager

Cyber Defense Infrastructure Support Specialist

Cyber Defense Incident Responder

Vulnerability Assessment Analyst

Threat/Warning Analyst

Exploitation Analyst

All-Source Analyst

Mission Assessment Specialist

Target Developer

Target Network Analyst

Multi-Disciplined Language Analyst

All Source-Collection Manager

All Source-Collection Requirements Manager

Cyber Intel Planner

Cyber Ops Planner

Partner Integration Planner

Cyber Operator

Cyber Crime Investigator

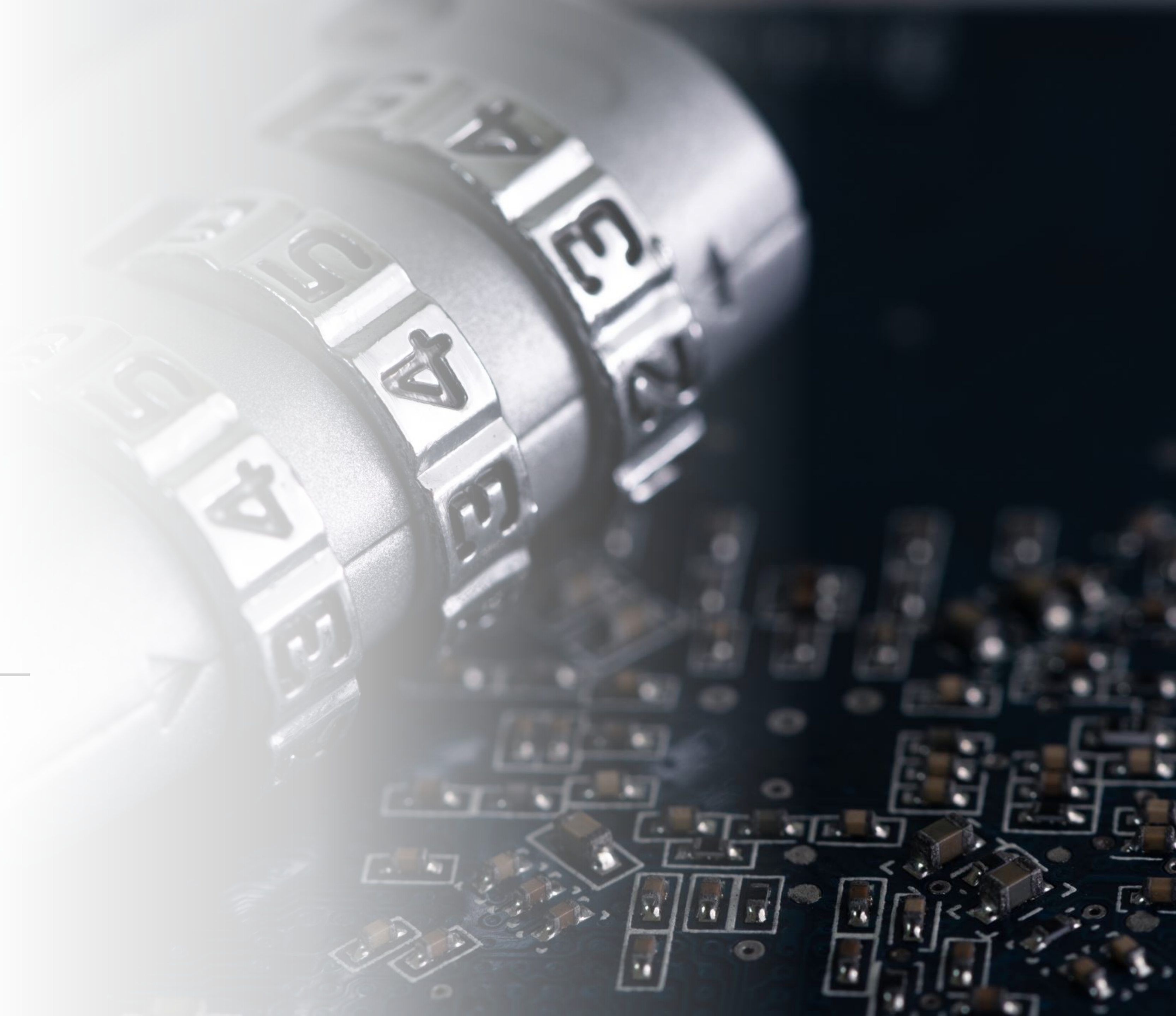
Law Enforcement /CounterIntelligence Forensics Analyst

Cyber Defense Forensics Analyst

Reasons for this Disconnect

- It is **difficult** to impossible for a single class or instructor **to provide a contextual expe**rience both in terms of a realistic environment as a realistic job role and tasks to be accomplished.
- Students graduate with component skills but are not given the opportunity to interact with an environment that will be akin to the one they might experience in the workforce.
- Because many **skills are taught in isolation** of other skills (Linux, Windows, networking devices, coding, etc) those skills may be lost and forgotten by the time of graduation.

Cybersecurity Capstone Project



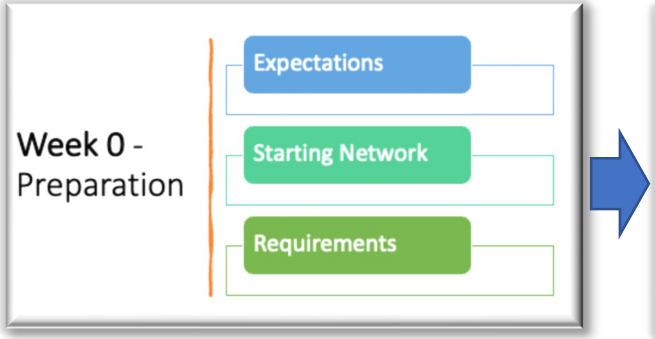
Capstone Class at CSUSB

NCYTE Cyber Career Challenge

Cybersecurity Capstone Project

- Provide students with
  - **Realistic experience** performing tasks related to work roles
  - Opportunity to **work in teams**
  - Opportunity to **discover** their **strengths** and **weaknesses** as well as their **interests**
  - Experiences that can help them secure employment in cybersecurity
  - **100% online** – meet twice weekly via zoom
  - Have **1 GA, 1-2 Volunteer** student assistants
  - Week 13 **pen tested** and operated by my **pen testing class**
  - Taken two forms – Capstone, cyber career challenge – NCYTE
  - Just had a small group of about 7 teachers go through the training
    - Teacher, trainer, student here questions at the end
  - **Dog park** – create situation where learning will occur
  - **Where there is interest there is learning**
  - **Teacher in role as manager** – remembers a few things from way back when

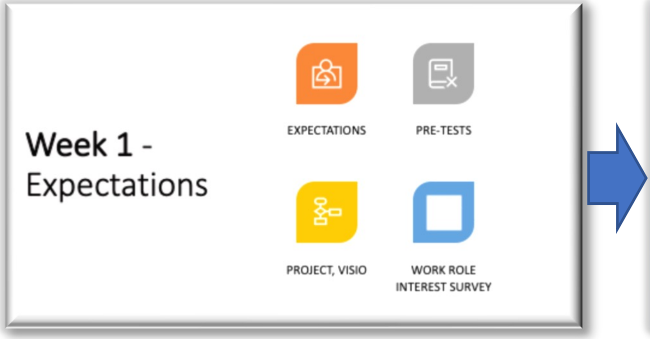
Capstone Progression


Week 0 - Preparation

Expectations

Starting Network

Requirements

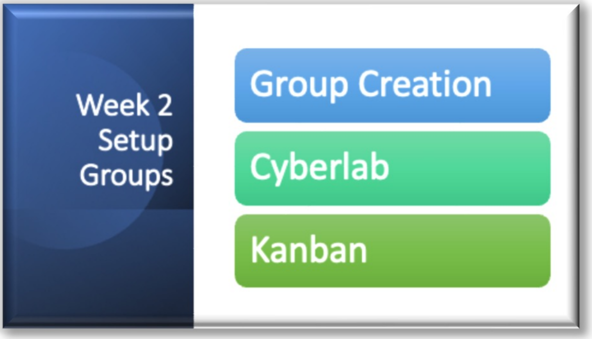

Week 1 - Expectations

EXPECTATIONS

PRE-TESTS

PROJECT, VISIO

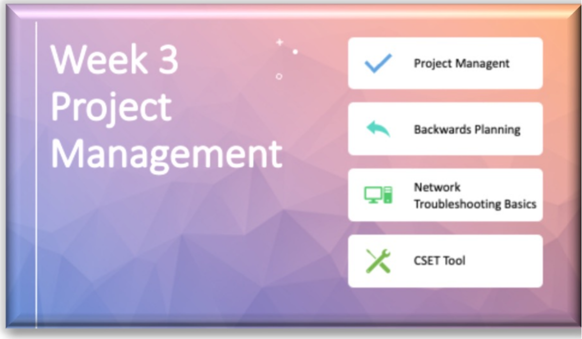
WORK ROLE INTEREST SURVEY


Week 2 Setup Groups

Group Creation

Cyberlab

Kanban

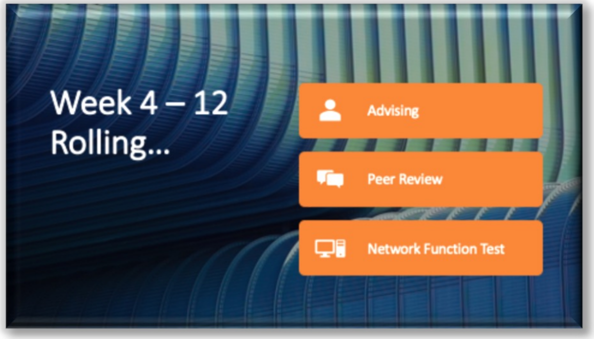

Week 3 Project Management

Project Managent

Backwards Planning

Network Troubleshooting Basics

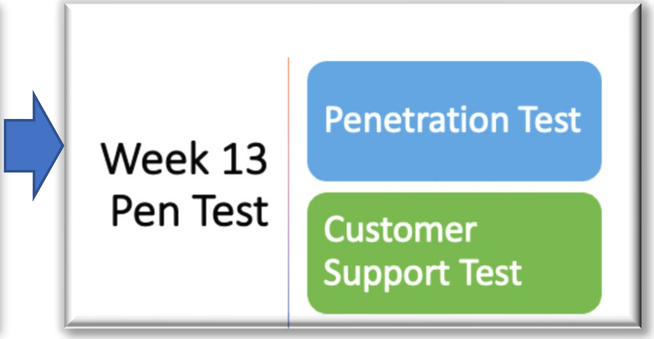
CSET Tool


Week 4 – 12 Rolling…

Advising

Peer Review

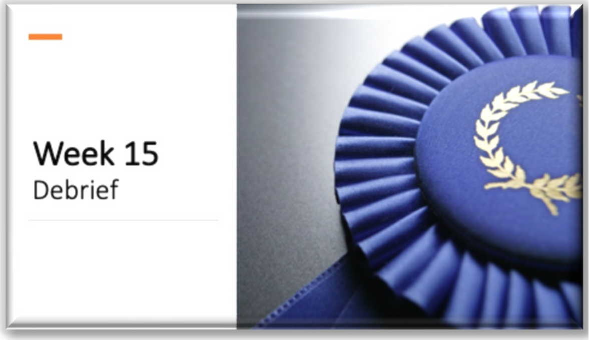
Network Function Test


Week 13 Pen Test

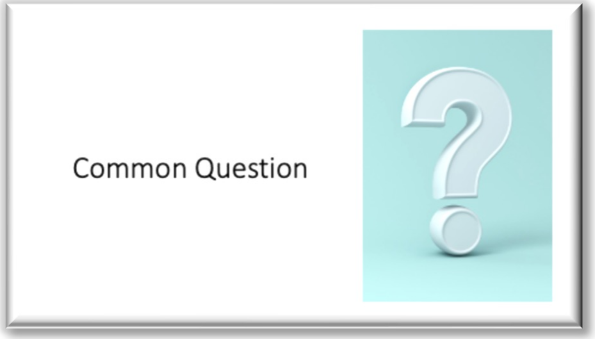
Penetration Test

Customer Support Test

Week 14 - Presentations


Week 15 Debrief

Results


Common Question

Q&A

Week 0 - Preparation

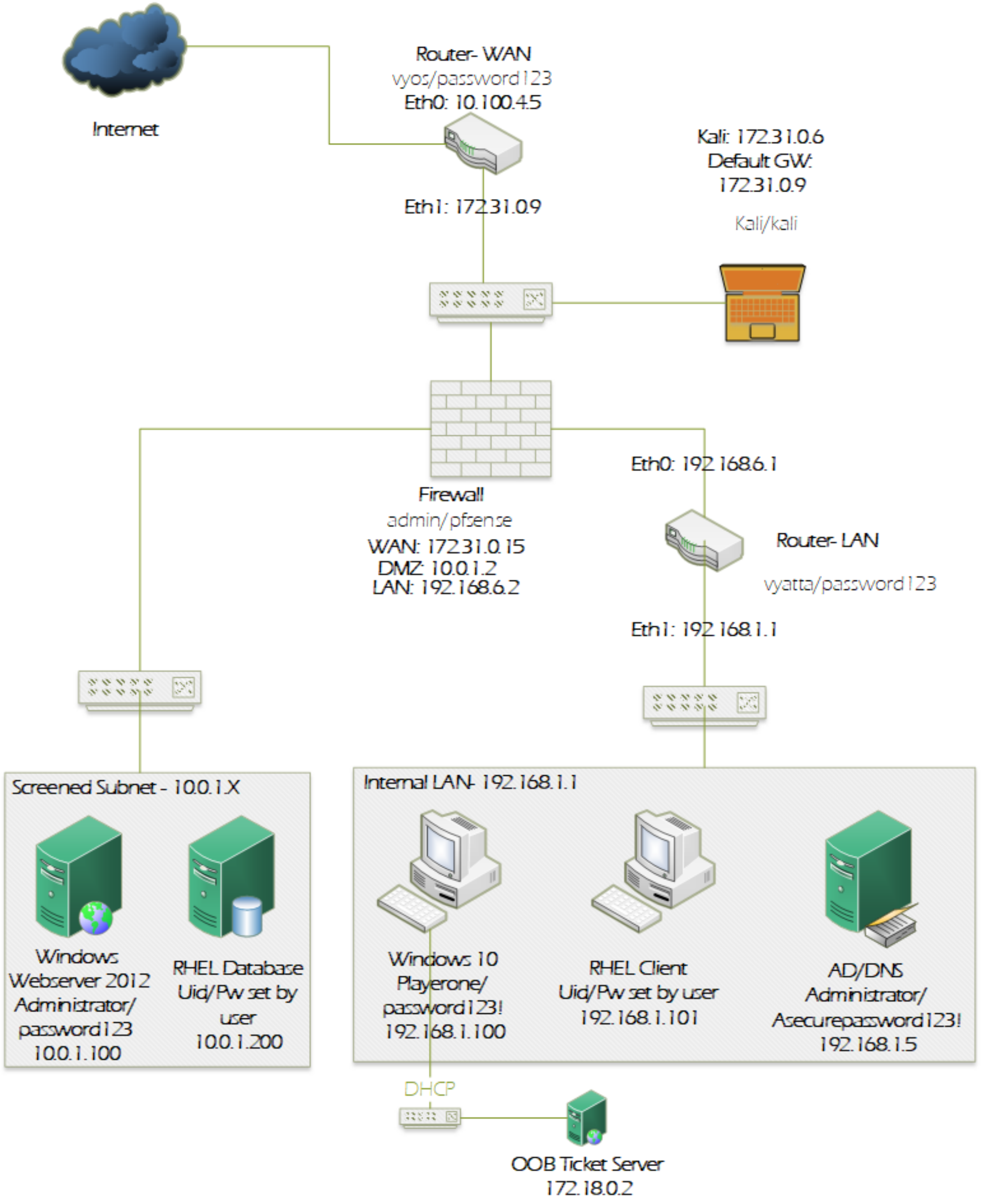
- Expectations
- Starting Network
- Requirements

Expectations

- Make clear that this is a capstone
    - Culminating activity of all your course work up until now
    - Will need to draw upon from courses you have taken in the program
    - Will require team work
    - Will require self learning
    - Meeting with your team outside of class
    - Not a procedural class

Starting Network

- 3 segment
- Full rights
- Teams of 3



	Task	Measure
Business Concept		
	Identified three goods	List of items submitted
	Identified three services	List of items submitted
Project Management		
	Gantt Chart	Completed Chart Posted
	Visio diagram of network	Diagram is accurate - information is correct
	FedRAMP System Security Plan	Accurate and complete
Account Management		
	Network authentication	Access the network admin console
	Admin account	Log in as admin
	User accounts	Log in as user
	Guest user account(such as consultant)	log in as a guest user
Web Management		
	Web site created	Access website from browser
	Shopping cart	access shopping cart on website
	purchase goods	purchase a good
	Purchase service	purchase a service
Database Management		
	Database setup	Access database interface
	Query db re goods	Query database for list of goods and other queries
Email		
	Email server setup	Access the email server admin interface
	User accounts get email access	Create a new user. Test email account.
	users can email each other from within organization	Compose and send email to other user. Check that it is received.
Scripting		
	Automate admin tasks with python	Script is run and behaves as intended
Workstations		
	1 Windows 1 Red Hat	
	Users can access/authenticate to network	Authenticate as any user and access network as appropriate
	Users can email	Compose and send email to other user. Check that it is received.
	Access to website/helpdesk	Open browser to helpdesk, submit ticket successfully
	Access other services	ie, access database
	Appropriate software to do work	Run various applications to assess functionality
Analytics		
	Network monitoring	access information about network traffic

Week 1 - Expectations

EXPECTATIONS

PRE-TESTS

PROJECT, VISIO

WORK ROLE
INTEREST SURVEY

Expectations

- Iterate the expectations
- Encourage and challenge the students
- Watch video from prior semester’s final presentations
- Goal is to prepare you for the work force
- You will have a customized Certificate at the completion

Pretest – Hands-on

- 1 - Kali - kali:kali
- 2 - ubuntu server (hidden) IP address 172.16.1.5 , web, ftp, ssh
- 3 – router (hidden) - internet access 10.10.100.1
- Complete the following:
  - Connect to **ubuntu server web page**. Download the image you see there
  - **FTP to the server** anonymous - download the file there
  - **SSH to the server** - user1 with pass of user1pass - **download the file there**
  - **Connect to internet with the router**
  - **Upload to canvas** from kali - answer this question
  - What do all the IP Addresses of all the machines have in common?

Project and Visio

- Make sure students have access to their **portal.azure.com** account
  - Treasure trove of FREE and LICENSED software from Microsoft
  - MS Project and Visio are free for download for students
- Students sign up for **Redhat** account
  - Students work on the **RH 124** course concurrent to this project
  - Optionally can do 134
- Also **Vmware IT Academy** – Though not needed for course

“What do you want to be when you grow up?”

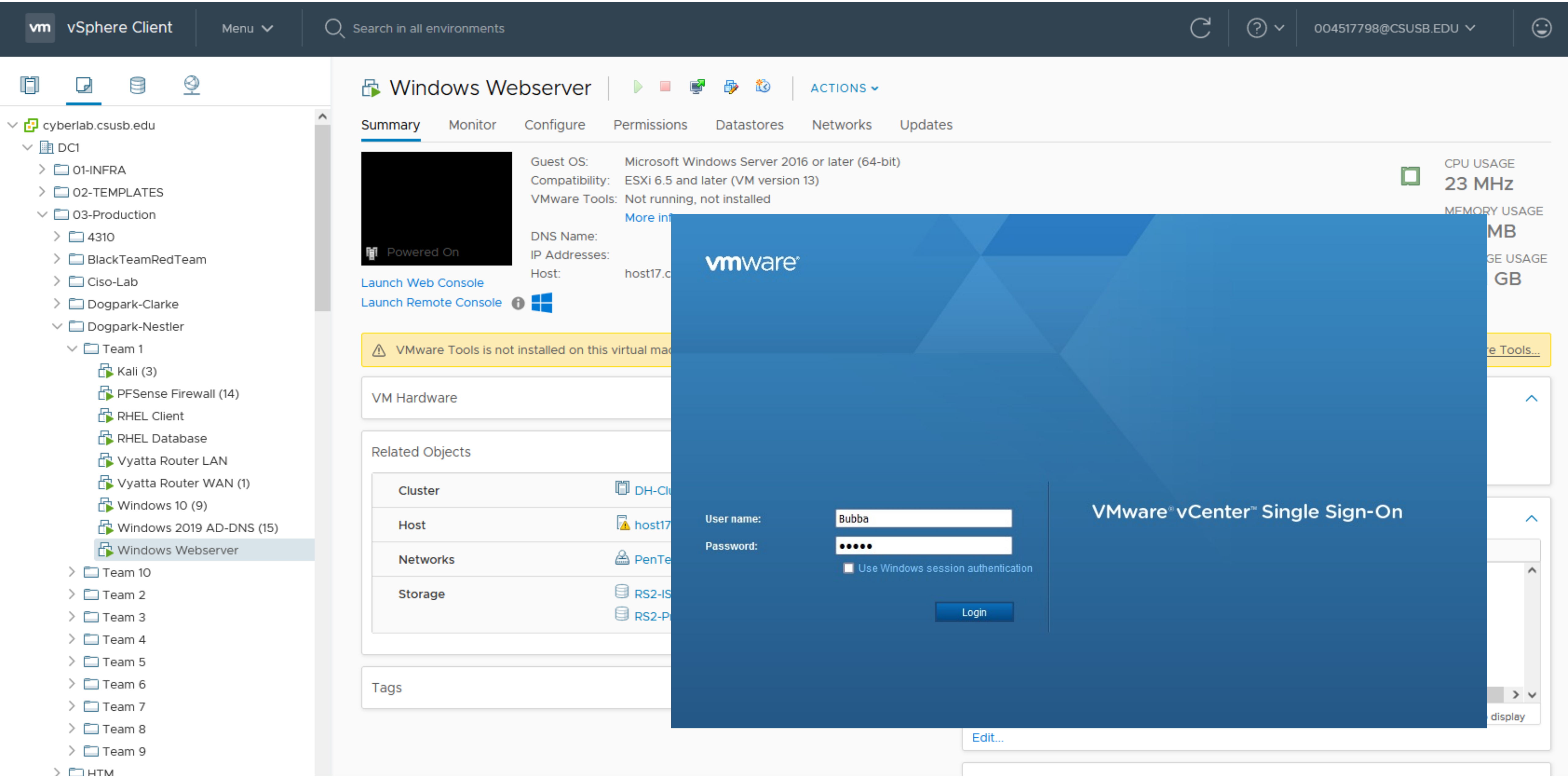
- Review all of the work roles
  - NICE Framework
    - https://cyberindustry.org/Workrole
    - https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool
  - DCWF
    - https://public.cyber.mil/wid/dcwf/
- List 3 work roles you are interested in.
- List three tasks for each work role you are interested in.
- This helps them determine their interest and it can help in selecting a balanced team.

Week 2 Setup Groups

- Group Creation
- Cyberlab
- Kanban

Group Creation

- Self Organized Learning Environments
  - Zoom using break out rooms
  - Students may choose their own groups, fill out spreadsheet for teams
  - Students may leave any group to go to another group, as long as it is unanimous
  - https://www.youtube.com/watch?v=dk60sYrU2RU&t=123s
- Put them in breakout rooms with their teams, establish times to meet and get contact information.
- Created Teams folder for each group to share files with each other and me.
- Share peer evaluation criteria (more later).



Guest OS: Microsoft Windows Server 2016 or later (64-bit)
Compatibility: ESXi 6.5 and later (VM version 13)
VMware Tools: Not running, not installed
More inf

DNS Name:
IP Addresses:
Host: host17.c

CPU USAGE
23 MHz
MEMORY USAGE
MB
GE USAGE
GB

⚠ VMware Tools is not installed on this virtual mac ... re Tools...

Cluster	DH-Cl
Host	host17
Networks	PenTe
Storage	RS2-IS RS2-P

vmware

VMware® vCenter™ Single Sign-On

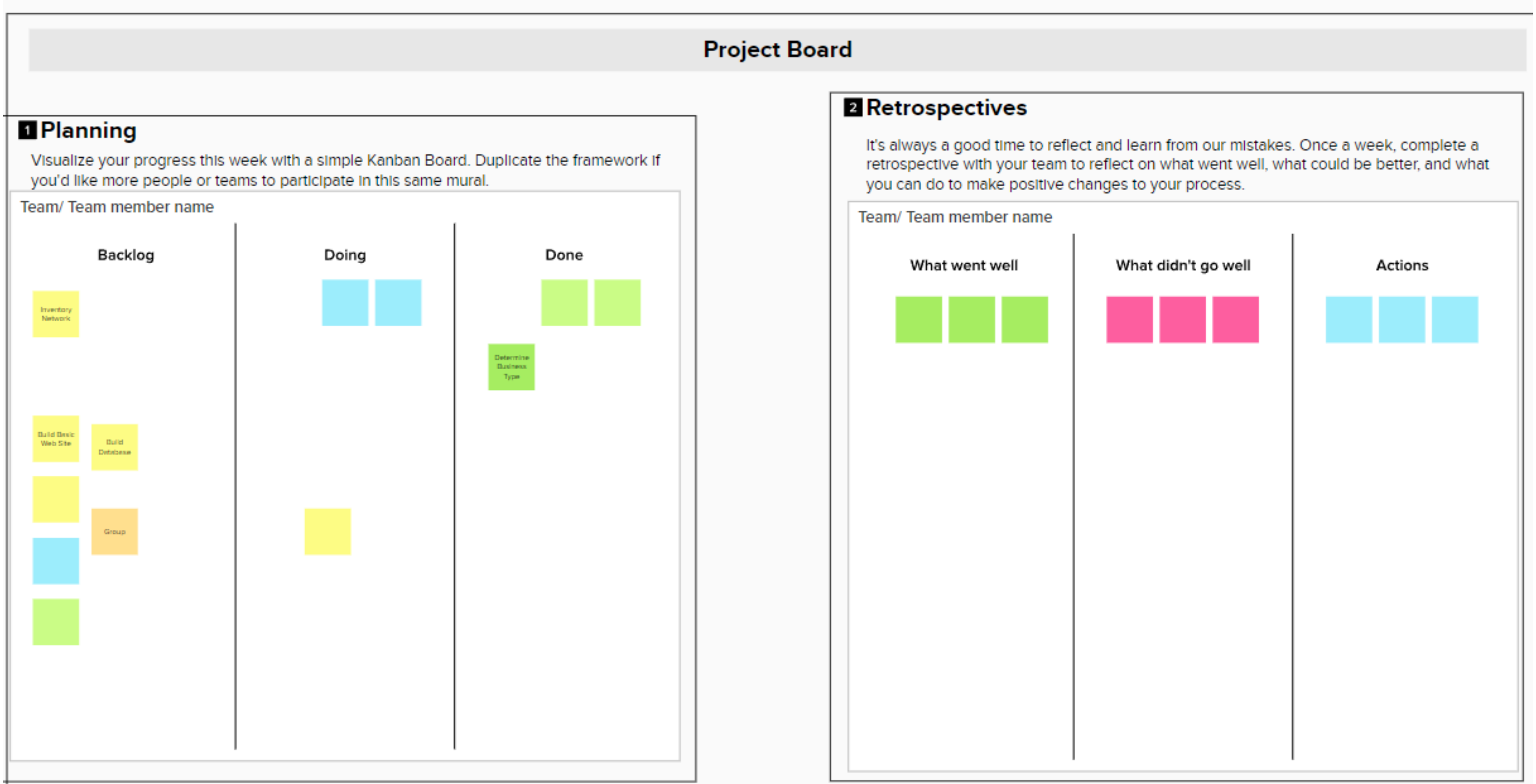
User name: Bubba

Password: •••••

□ Use Windows session authentication

Login

Kanban



Project Board

1 Planning

Visualize your progress this week with a simple Kanban Board. Duplicate the framework if you'd like more people or teams to participate in this same mural.

Team/ Team member name

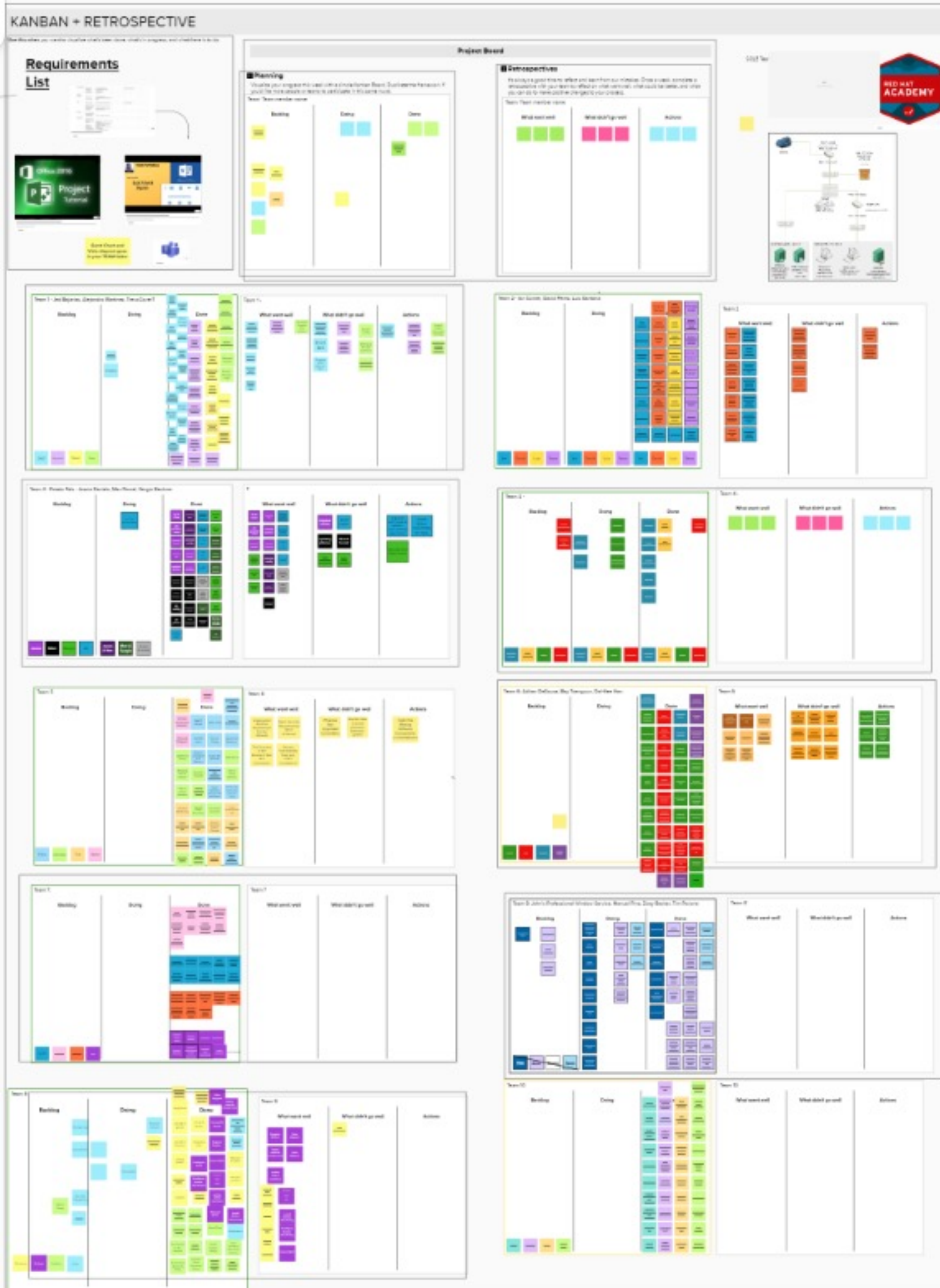
2 Retrospectives

It's always a good time to reflect and learn from our mistakes. Once a week, complete a retrospective with your team to reflect on what went well, what could be better, and what you can do to make positive changes to your process.

Team/ Team member name

Kanban Use

- One stop shop for project and resources.
- Used to manage the chaos.
- Tasks from requirements/project go here.
- Individuals color coded post-its.
- Must be maintained for each team daily, checked twice weekly.
- All teams can see other teams Kanbans. Encouraged to do so.
- May and should communicate with other teams.
- Used in part for the verification of certificates (more later).



Week 3 Project Management

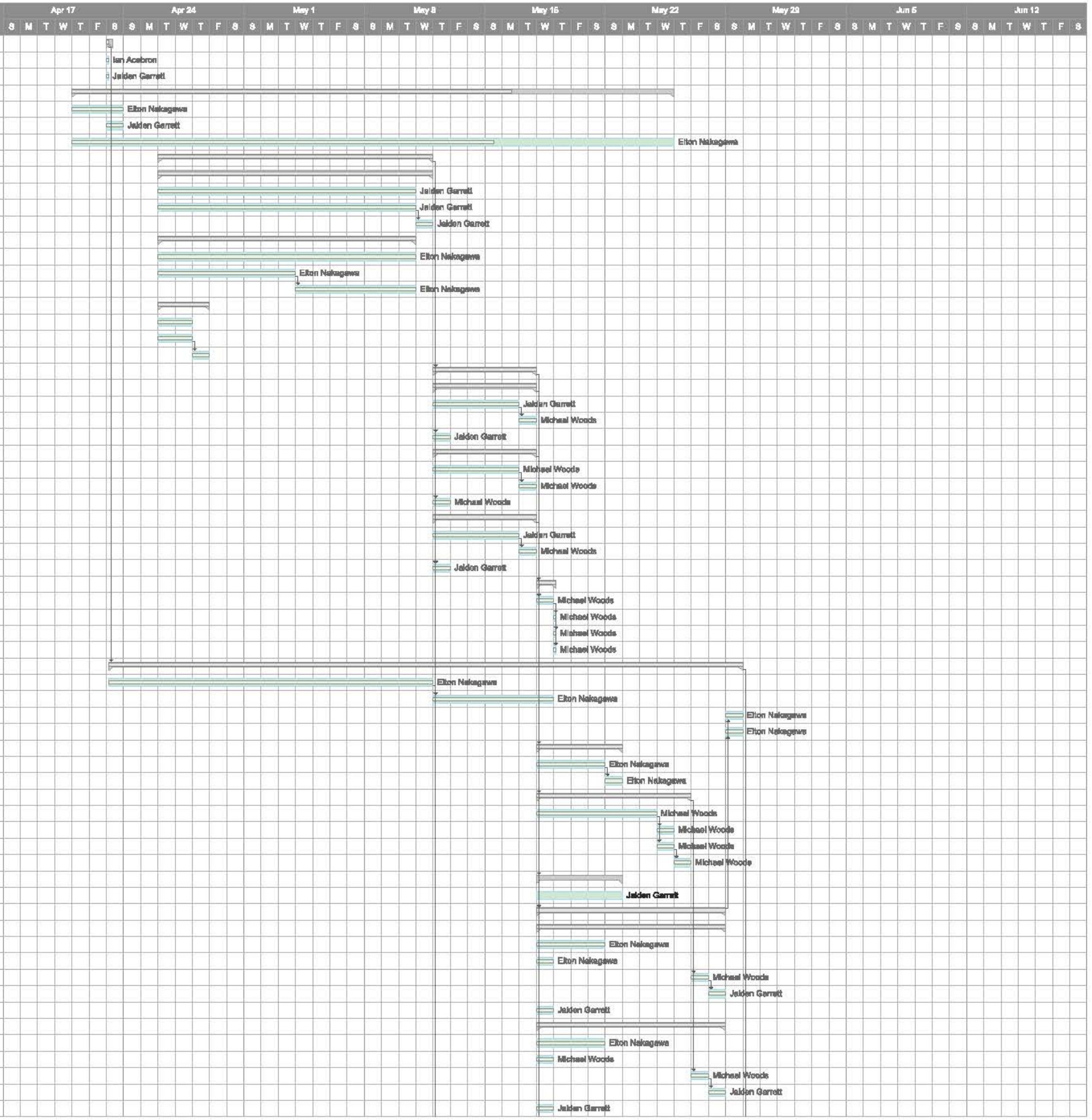
- ✓ Project Managent
- Backwards Planning
- Network Troubleshooting Basics
- CSET Tool

Backward Planning and Backwards Planning

- Your team is being pentested week 13. You must be done by week 12.
  - Plan backwards from there.
- List out all of your task from the requirements list.
  - Determine other tasks needed but not listed
  - Determine what tasks are dependent on others as predecessors
  - Assign the tasks to individuals

Team x Project

	Task Name	Duration	Start	Finish	Predecessors
1	Business Concept	0.125d	04/23/22	04/23/22	
2	Identify three goods	1h	04/23/22	04/23/22	
3	Identify three services	1h	04/23/22	04/23/22	
4	Project Management	35d	04/21/22	05/25/22	
5	Gantt chart	3d	04/21/22	04/23/22	
6	Visio diagram	1d	04/23/22	04/23/22	
7	CSET	35d	04/21/22	05/25/22	
8	Networking	16d	04/26/22	05/11/22	
9	Firewall	16d	04/26/22	05/11/22	
10	Check configs	15d	04/26/22	05/10/22	
11	Make adjustments if necessary	15d	04/26/22	05/10/22	
12	Update and set rules	1d	05/11/22	05/11/22	11
13	Routers	15d	04/26/22	05/10/22	
14	Check configs	15d	04/26/22	05/10/22	
15	Make adjustments if necessary	8d	04/26/22	05/03/22	
16	Update and set rules	7d	05/04/22	05/10/22	15
17	Switches	3d	04/26/22	04/28/22	
18	Check configs	2d	04/26/22	04/27/22	
19	Make adjustments if necessary	2d	04/26/22	04/27/22	
20	Update and set rules	1d	04/28/22	04/28/22	19
21	Servers	6d	05/12/22	05/17/22	8
22	Windows 2016 Server	6d	05/12/22	05/17/22	
23	Install software	5d	05/12/22	05/16/22	
24	Set system backup	1d	05/17/22	05/17/22	23
25	Network config and test	1d	05/12/22	05/12/22	8
26	AD/DNS Server	6d	05/12/22	05/17/22	
27	Install software	5d	05/12/22	05/16/22	
28	Set system backup	1d	05/17/22	05/17/22	27
29	Network config and test	1d	05/12/22	05/12/22	8
30	RHEL Database	6d	05/12/22	05/17/22	
31	Install software	5d	05/12/22	05/16/22	
32	Set system backup	1d	05/17/22	05/17/22	31
33	Network config and test	1d	05/12/22	05/12/22	8
34	Account Management	1.125d	05/18/22	05/19/22	28
35	Network authentication	1d	05/18/22	05/18/22	28
36	Admin account	1h	05/19/22	05/19/22	35
37	User accounts	1h	05/19/22	05/19/22	35
38	Guest user	1h	05/19/22	05/19/22	35
39	Web Management	36.875d	04/23/22	05/29/22	1
40	Website creation	18.875d	04/23/22	05/11/22	
41	Shopping cart	7d	05/12/22	05/18/22	40
42	Purchase goods test	1d	05/29/22	05/29/22	54
43	Purchase services test	1d	05/29/22	05/29/22	54
44	Database Management	5d	05/18/22	05/22/22	30
45	Database setup	4d	05/18/22	05/21/22	
46	Query testing	1d	05/22/22	05/22/22	45
47	Email	9d	05/18/22	05/26/22	22
48	Email server setup	7d	05/18/22	05/24/22	
49	Set backup system	1d	05/25/22	05/25/22	48
50	Create user accounts	1d	05/25/22	05/25/22	48
51	Email testing	1d	05/26/22	05/26/22	50
52	Scripting	5d	05/18/22	05/22/22	21
53	Automate admin tasks with python	5d	05/18/22	05/22/22	
54	Workstations	11d	05/18/22	05/28/22	21
55	Windows Setup	11d	05/18/22	05/28/22	
56	Software installation	4d	05/18/22	05/21/22	
57	Authentication test	1d	05/18/22	05/18/22	
58	Email test	1d	05/27/22	05/27/22	47
59	Helpdesk test	1d	05/28/22	05/28/22	58
60	Access other services	1d	05/18/22	05/18/22	
61	Red Hat Setup	11d	05/18/22	05/28/22	
62	Software installation	4d	05/18/22	05/21/22	
63	Authentication test	1d	05/18/22	05/18/22	
64	Email test	1d	05/27/22	05/27/22	47
65	Helpdesk test	1d	05/28/22	05/28/22	64
66	Access other services	1d	05/18/22	05/18/22	



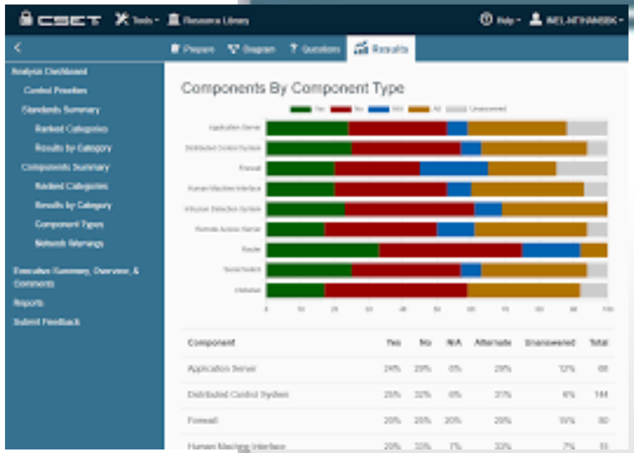
Exported on June 12, 2022 12:50:43 PM HST

Network Troubleshooting

- A quick course on networking basics and troubleshooting
- IP addressing, Routing (reverse routes).
- Tools – ping, ip, tcpdump, tshark, tracert, nslookup, etc
- Shared collection of “cheatsheets”
  - Nmap, linux, vyos, pfsense, etc

CSET®

CYBER SECURITY EVALUATION TOOL



Components By Component Type

Component	Yes	No	N/A	Alternate	Unanswered	Total
Application Server	24%	29%	0%	29%	12%	66
Distributed Control System	25%	32%	0%	31%	6%	144
Firewall	20%	25%	20%	20%	15%	80
Human Machine Interface	20%	33%	7%	33%	7%	11

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA
CYBER+INFRASTRUCTURE

RRA Performance Summary

These charts represent the answer distribution overall and across all tiers.

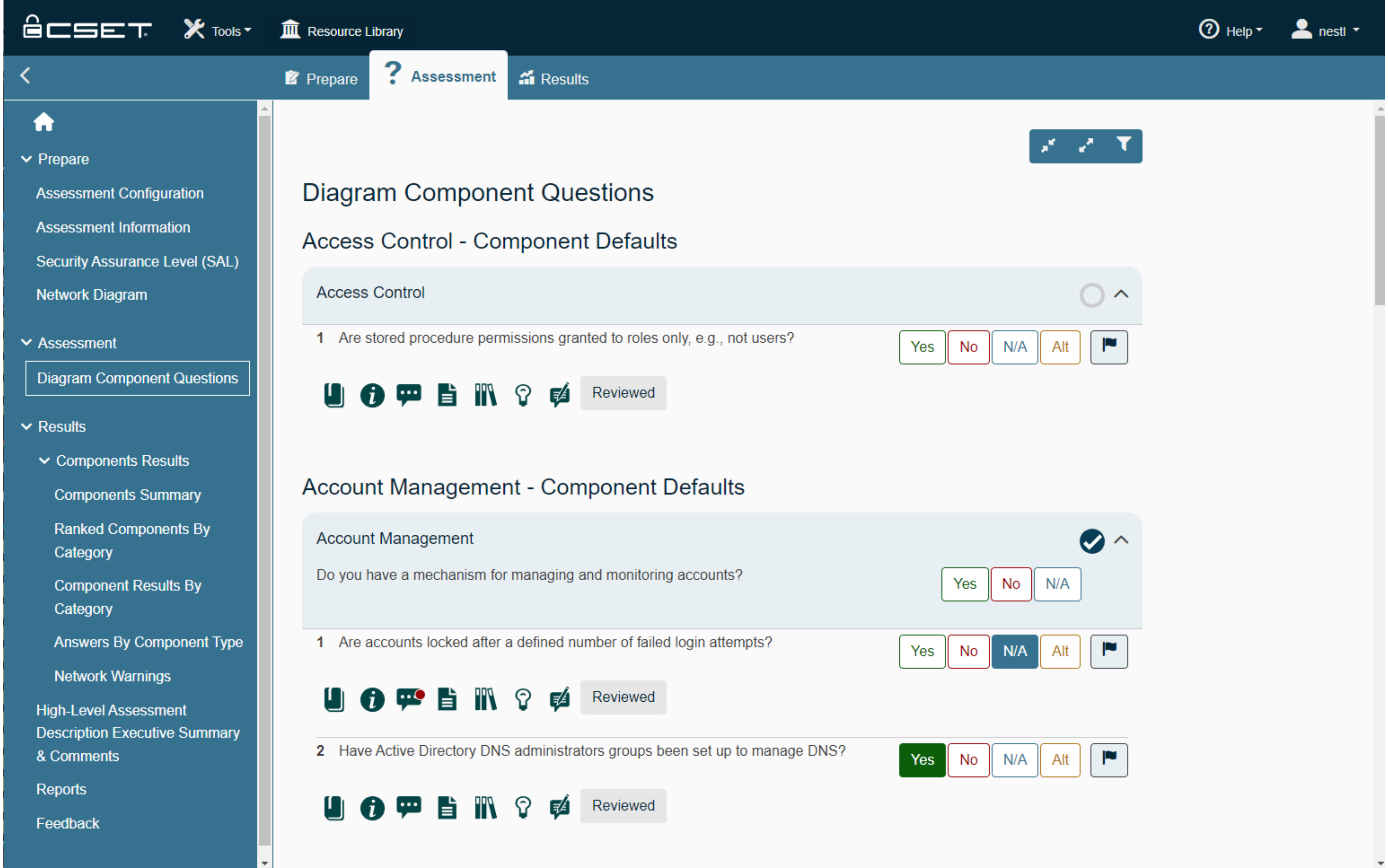


Diagram Component Questions

Access Control - Component Defaults

Access Control

1 Are stored procedure permissions granted to roles only, e.g., not users? Yes No N/A Alt

Account Management - Component Defaults

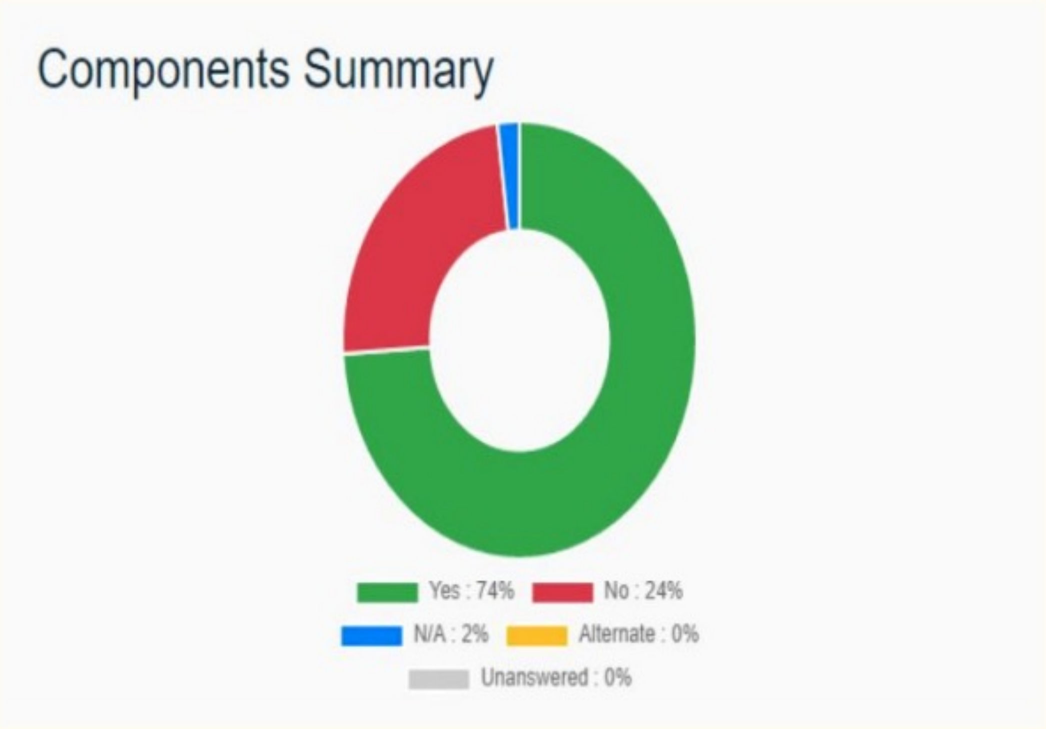
Account Management

Do you have a mechanism for managing and monitoring accounts? Yes No N/A

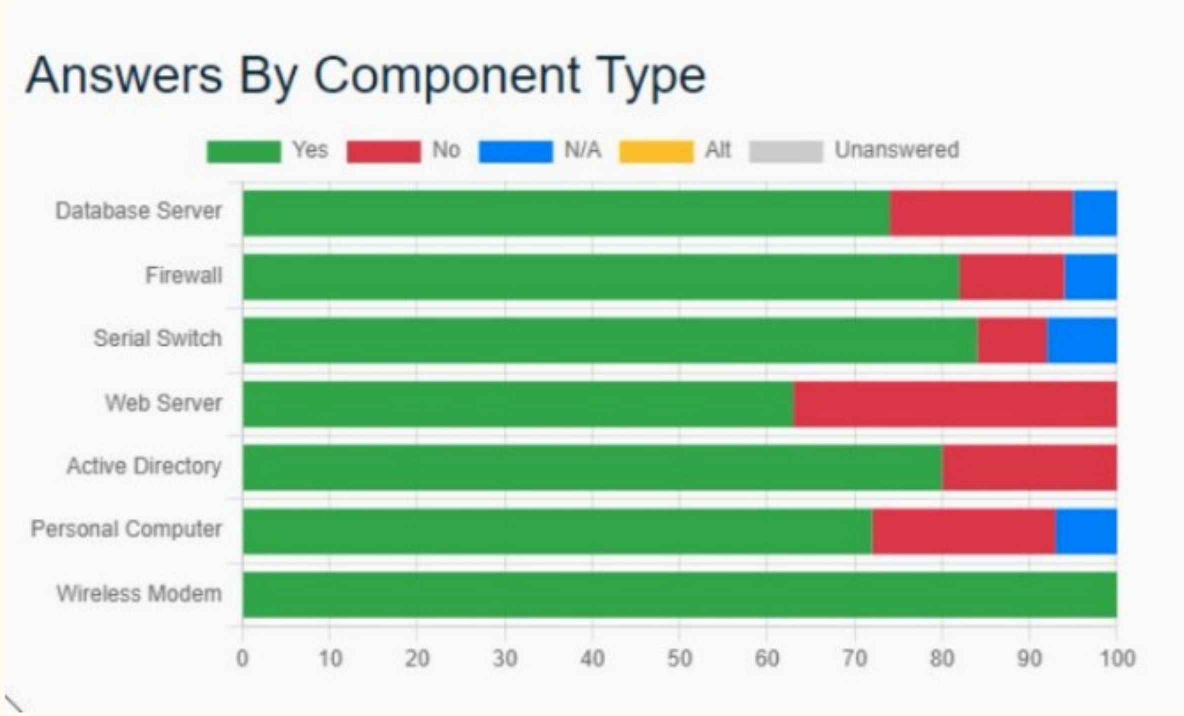
1 Are accounts locked after a defined number of failed login attempts? Yes No [✓ N/A] Alt

2 Have Active Directory DNS administrators groups been set up to manage DNS? [✓ Yes] No N/A Alt

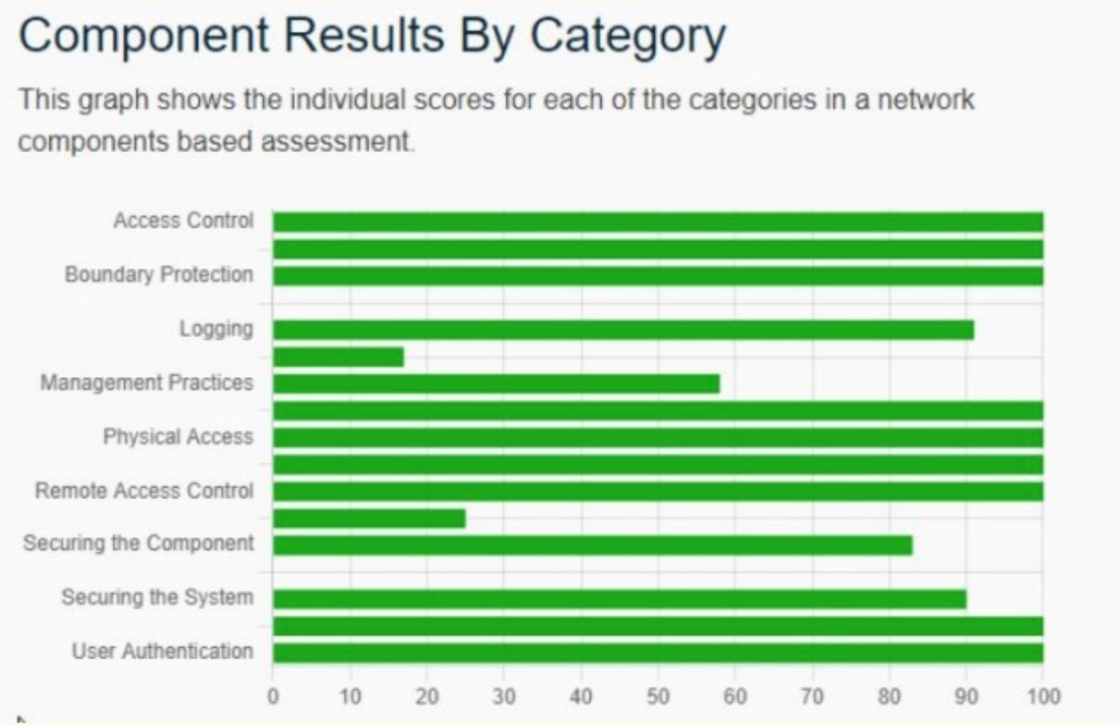
CSET Summary



CSET Cyber Assessment: The cyber assessment is used to evaluate our organization's operational resilience and our networks cybersecurity practices.

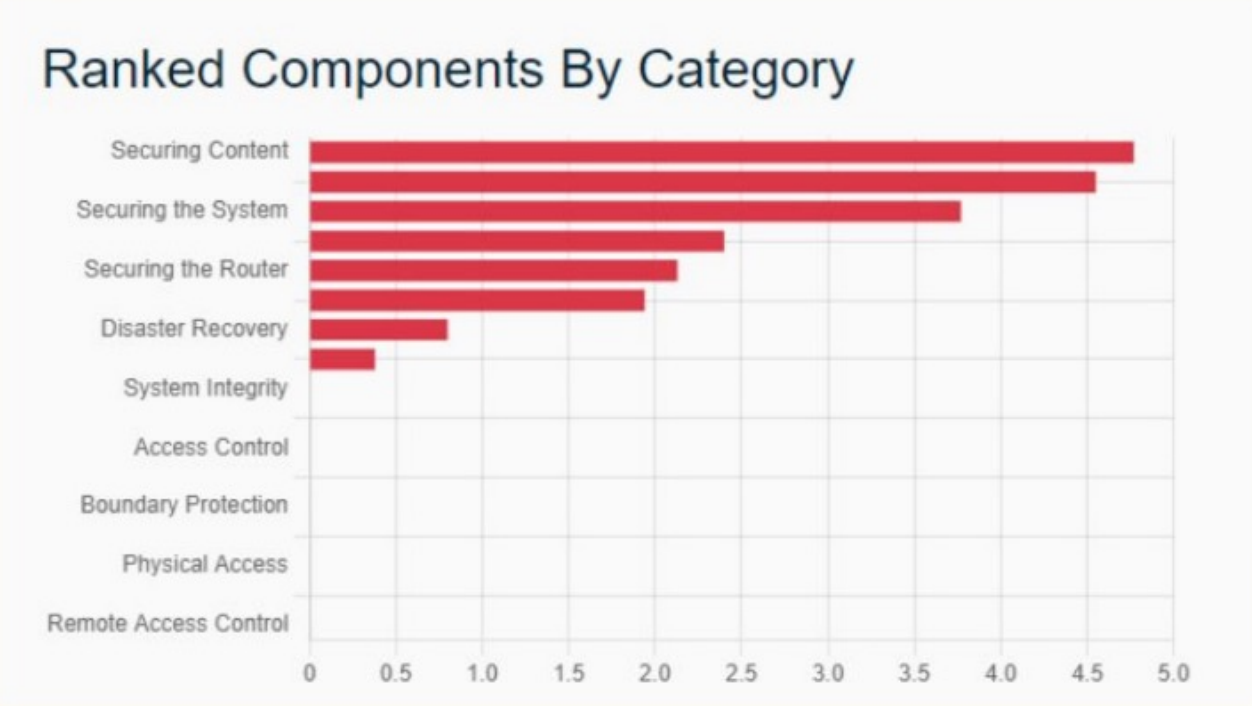


CSET Results Continued



Component Results By Category

This graph shows the individual scores for each of the categories in a network components based assessment.



Ranked Components By Category

Standards Strengths:

- ★ Access Control
- ★ Remote Access Control
- ★ Logging

Questions of Concern:

- ★ Securing the content (putting logs, OS, Database in separate partitions
- ★ Securing the content (didn't put blocks on opening folders, make error logs vague)
- ★ Securing the router (did not disallow invalid incoming addresses, did not put warning of criminal charges if messed with)

Week 4 – 12 Rolling…

- Advising
- Peer Review
- Network Function Test

Advising

- Each week after short information sharing, into breakout rooms
- Go to each team
- Share wisdom
  - How do you eat an elephant?
  - Don’t let what you can't do stop from doing what you can do
  - It is always darkest before dawn
  - Try to think two levels above you
  - If it is not in writing it did not happen
  - Answer the question I asked please.
  - Be more precise in what you are saying.

Peer Review

- Peer review distributed via Qualtrics link
- Peer Review Questionnaire
  - The student showed they were prepared during group meetings.
  - The student was punctual to meetings.
  - The student was open and receptive to the opinions and suggestions of others.
  - The student was engaged during group meetings and discussions.
  - The student worked collaboratively within the team.
  - The student was able to come up with solutions to problems and challenges the team faced.
  - The student accepted and responded appropriately to criticism and feedback.
  - The student was able to communicate their ideas clearly.
  - Overall the student contributed to the progress and development of the team mission.

- Given at mid term (week 8) and at the end (Week 16)
- All questions – 5 point Likert Scale
- Questions came from:
  - https://bmcmededuc.biomedcentral.com/articles/10.1186/s12909-021-02821-6

1	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree
1	Neither agree nor disagree	Somewhat disagree	Somewhat agree	Neither agree nor disagree	Somewhat agree	Somewhat agree	Strongly agree	Somewhat agree	Somewhat disagree
1	Neither agree nor disagree	Neither agree nor disagree	Somewhat agree	Somewhat disagree	Neither agree nor disagree	Somewhat disagree	Neither agree nor disagree	Neither agree nor disagree	Neither agree nor disagree
1	Neither agree nor disagree	Somewhat disagree	Neither agree nor disagree	Somewhat disagree	Neither agree nor disagree	Somewhat disagree	Neither agree nor disagree	Neither agree nor disagree	Neither agree nor disagree
1	Somewhat agree	Somewhat disagree	Strongly agree	Somewhat disagree	Neither agree nor disagree	Strongly agree	Strongly agree	Somewhat agree	Neither agree nor disagree
2	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree
2	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree
2	Strongly agree	Somewhat agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree
2	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree	Strongly agree

Network Function Test

- Week 12 Orange teams check networks
  - Workstations
    - Have required software – office suite
  - Given domain accounts to access both workstations
    - Windows 10
    - Redhat
  - Web server is up
    - Business site is accessible
    - Goods are posted
    - Shopping cart “works”
    - Ticket system is up
    - Dashboard is up
  - Email server is up
    - Able to email internally
    - PKI – encrypted email as well
    - site is up

Comes from original requirements Doc

Week 13
Pen Test

Penetration Test

Customer Support Test

Penetration Test

- Ethical hacking class pentests the capstone class
- The ethical hacking class should be the class taken prior to the capstone class
- Red team has specific playbook to run
- Red team also produces a report – Template
- Orange team purchases items, changes orders, creates trouble tickets

Week 14 - Presentations

Presentation Template

- Intro Slide
- Gantt Chart
- Network diagram with notes on significant modifications
- Auditing and Compliance
- Pentest results analysis from their perspective
- Customer Service from their perspective
- **Report from orange and red team**
- Lessons learned

Presentation Survey

- **Gantt Chart** was clear and succinct
- **Network Diagram** was clear and succinct
- **Detection and Analysis** was clear and succinct
- **Auditing and Compliance** was clear and succinct
- **Pentest Week Analysis and Service** was clear and succinct
- **Lessons Learned** was clear and succinct

Week 15

Debrief

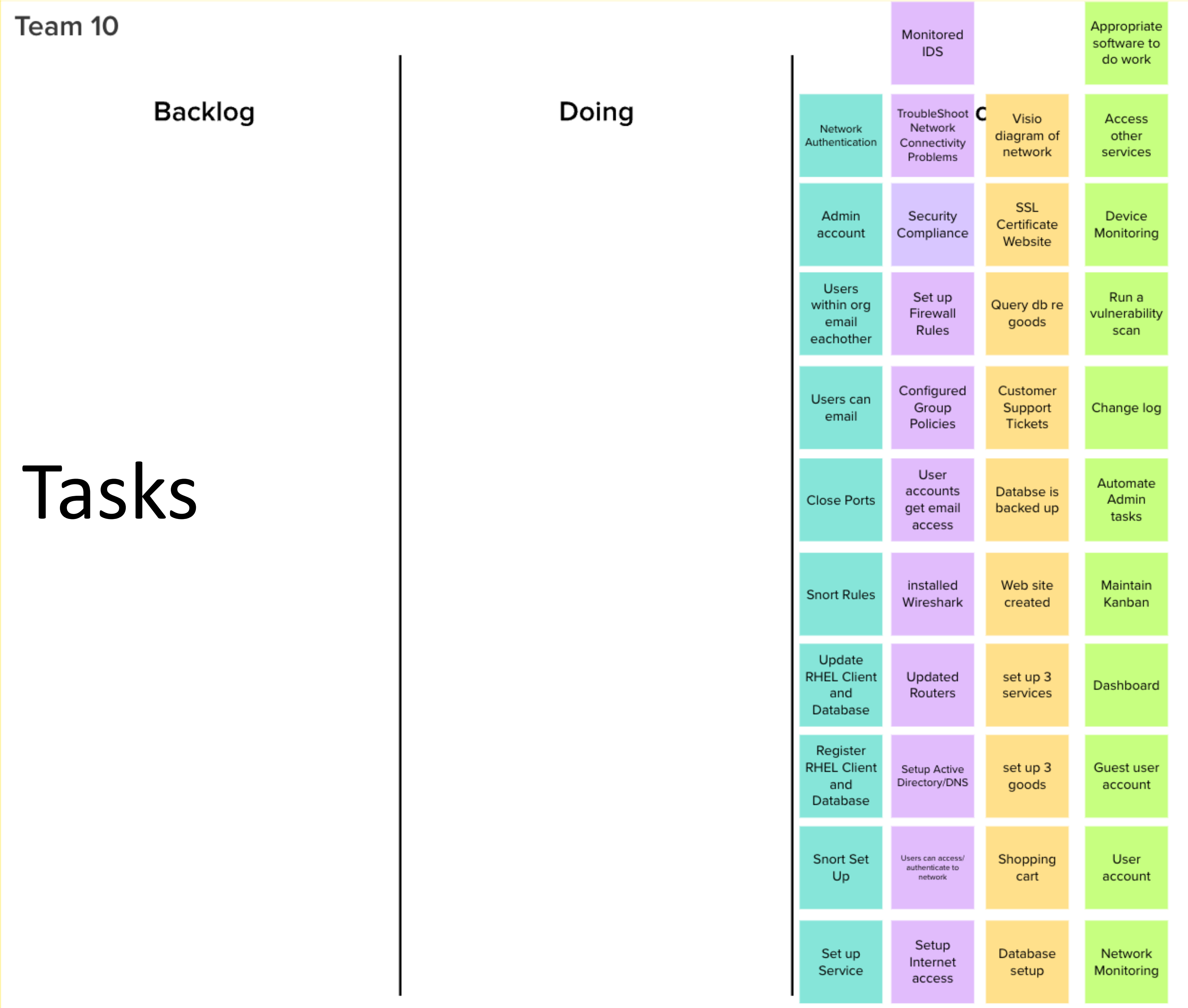
Debrief

- Discussion with student on their experience
- Exit Survey
- Feed back

STAR Method

- Have the students practice explaining their experience in the capstone, given a prompt from an interviewer
    - Share an experience where you were facing a difficult situation in a team and how you handled it.
- S – Situation
- T – Task
- A – Action
- R - Result

Final Kanban Tasks



Team 10

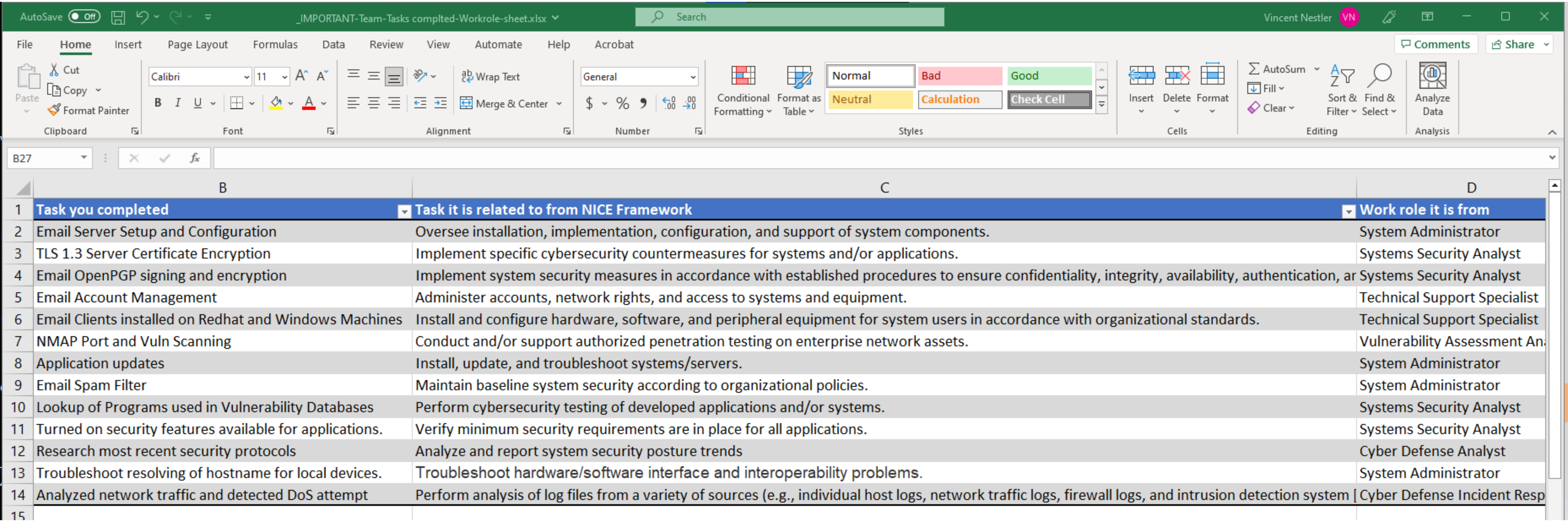
Backlog

Doing

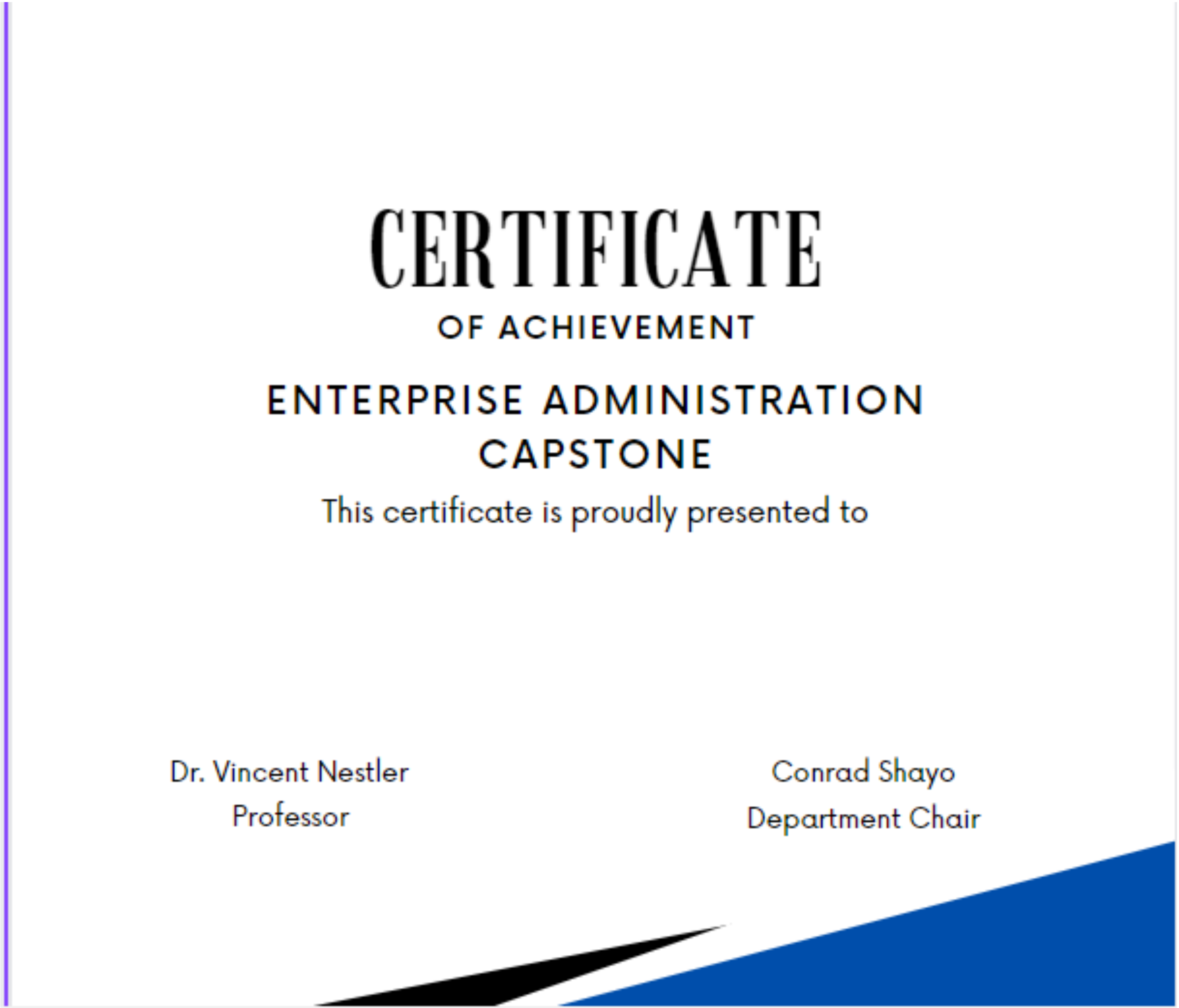
C

	Monitored IDS		Appropriate software to do work
Network Authentication	TroubleShoot Network Connectivity Problems	Visio diagram of network	Access other services
Admin account	Security Compliance	SSL Certificate Website	Device Monitoring
Users within org email eachother	Set up Firewall Rules	Query db re goods	Run a vulnerability scan
Users can email	Configured Group Policies	Customer Support Tickets	Change log
Close Ports	User accounts get email access	Databse is backed up	Automate Admin tasks
Snort Rules	installed Wireshark	Web site created	Maintain Kanban
Update RHEL Client and Database	Updated Routers	set up 3 services	Dashboard
Register RHEL Client and Database	Setup Active Directory/DNS	set up 3 goods	Guest user account
Snort Set Up	Users can access/ authenticate to network	Shopping cart	User account
Set up Service	Setup Internet access	Database setup	Network Monitoring

Task Completion Spreadsheet



	B	C	D
1	Task you completed	Task it is related to from NICE Framework	Work role it is from
2	Email Server Setup and Configuration	Oversee installation, implementation, configuration, and support of system components.	System Administrator
3	TLS 1.3 Server Certificate Encryption	Implement specific cybersecurity countermeasures for systems and/or applications.	Systems Security Analyst
4	Email OpenPGP signing and encryption	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, ar	Systems Security Analyst
5	Email Account Management	Administer accounts, network rights, and access to systems and equipment.	Technical Support Specialist
6	Email Clients installed on Redhat and Windows Machines	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	Technical Support Specialist
7	NMAP Port and Vuln Scanning	Conduct and/or support authorized penetration testing on enterprise network assets.	Vulnerability Assessment An
8	Application updates	Install, update, and troubleshoot systems/servers.	System Administrator
9	Email Spam Filter	Maintain baseline system security according to organizational policies.	System Administrator
10	Lookup of Programs used in Vulnerability Databases	Perform cybersecurity testing of developed applications and/or systems.	Systems Security Analyst
11	Turned on security features available for applications.	Verify minimum security requirements are in place for all applications.	Systems Security Analyst
12	Research most recent security protocols	Analyze and report system security posture trends	Cyber Defense Analyst
13	Troubleshoot resolving of hostname for local devices.	Troubleshoot hardware/software interface and interoperability problems.	System Administrator
14	Analyzed network traffic and detected DoS attempt	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [	Cyber Defense Incident Resp
15			



CERTIFICATE

OF ACHIEVEMENT

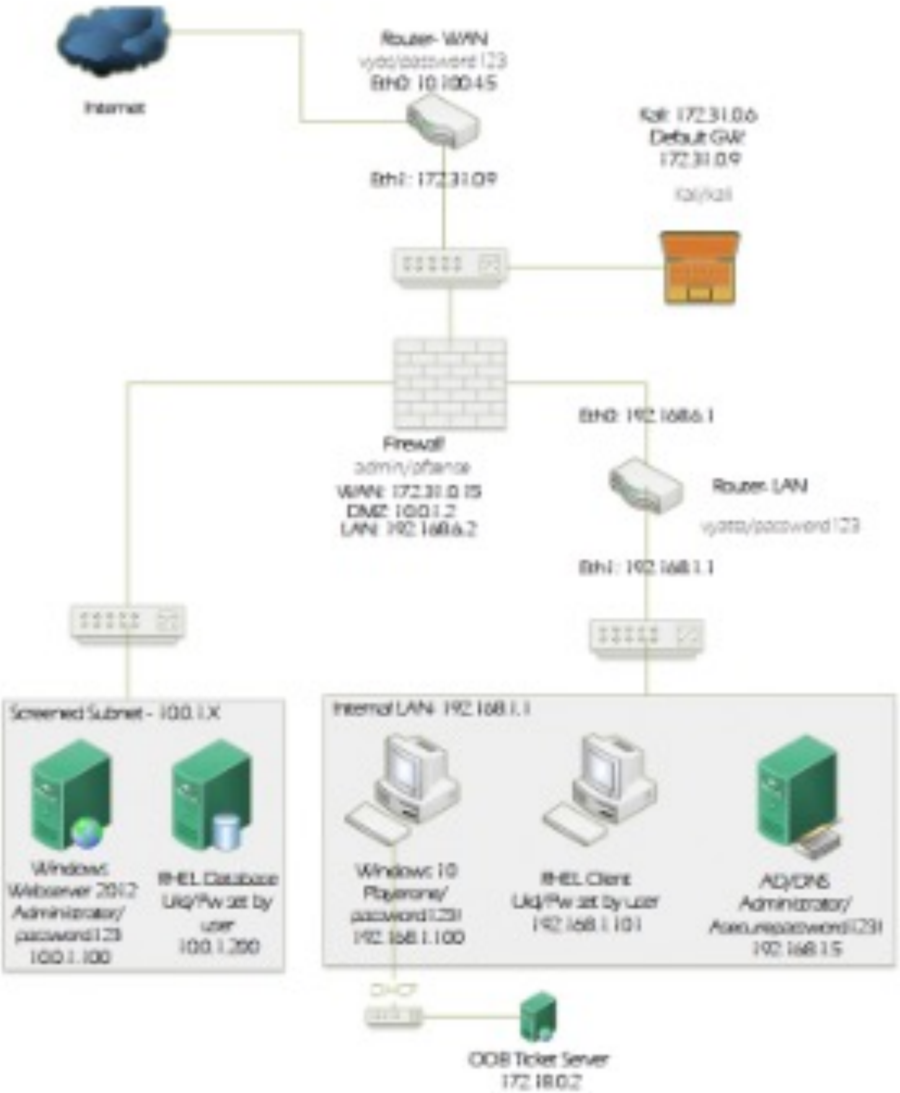
ENTERPRISE ADMINISTRATION CAPSTONE

This certificate is proudly presented to

Dr. Vincent Nestler
Professor

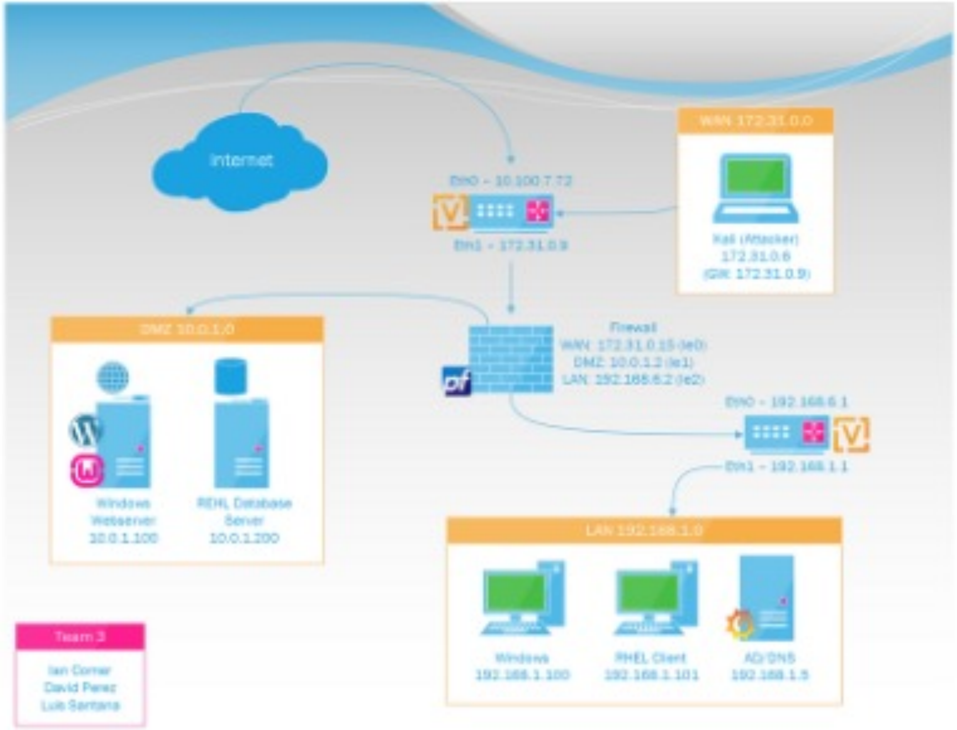
Conrad Shayo
Department Chair

The capstone experience is designed to give participants the opportunity to gain important workforce experience before entering the workforce. Participants work on a small business network (diagram below) in teams of 3 or 4. The teams are given a list of requirements (listed below) that they must complete by the date of allowing user access and being the subject of a week long penetration test. The results of the experience and the list of specific tasks the participant completed is listed on the next page along with the diagram and modifications made to the network.



Business Concept		
	Identified three goods	List of items submitted
	Identified three services	List of items submitted
Project Management		
	Gantt Chart	Completed Chart Posted
	Visio diagram of network	Diagram is accurate - information is correct
	FedRAMP System Security Plan	Accurate and complete
Account Management		
	Network authentication	Access the network admin console
	Admin account	Log in as admin
	User accounts	Log in as user
	Guest user account (such as consultant)	log in as a guest user
Web Management		
	Web site created	Access website from browser
	Shopping cart	access shopping cart on website
	purchase goods	purchase a good
	Purchase service	purchase a service
Database Management		
	Database setup	Access database interface
	Query db re goods	Query database for list of goods and other queries

Final Network - Below is the network diagram as it was modified and a list of some of the tasks completed in support of the development of this network.



Completed Task	Related NICE Framework Task	Work Role
Email Server Setup and Configuration	Oversee installation, implementation, configuration, and support of system components.	System Administrator
TLS 1.3 Server Certificate Encryption	Implement specific cybersecurity countermeasures for systems and/or applications.	Systems Security Analyst
Email OpenPGP signing and encryption	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.	Systems Security Analyst
Email Account Management	Administer accounts, network rights, and access to systems and equipment.	Technical Support Specialist
Email Clients installed on Redhat and Windows Machines	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	Technical Support Specialist
NMAP Port and Vuln Scanning	Conduct and/or support authorized penetration testing on enterprise network assets.	Vulnerability Assessment Analyst
Application updates	Install, update, and troubleshoot systems/servers.	System Administrator
Email Spam Filter	Maintain baseline system security according to organizational policies.	System Administrator
Lookup of Programs used in Vulnerability Databases	Perform cybersecurity testing of developed applications and/or systems.	Systems Security Analyst
Turn on all security features available for applications.	Verify minimum security requirements are in place for all applications.	Systems Security Analyst
Research most recent security protocols	Analyze and report system security posture trends	Cyber Defense Analyst
Troubleshoot resolving of hostname for local devices.	Troubleshoot hardware/software interface and interoperability problems.	System Administrator
Analyzed network traffic and detected DoS attempt	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system (IDS) logs) to identify possible threats to network security.	Cyber Defense Incident Responder

Results

Some Results From Surveys

- Top Work Roles of Interest
  - Cyber Defense Analyst
  - System Administrator
  - Cyber Crime Investigator
  - Cyber Incident Responder
  - Vulnerability Assessment Analyst
  - System Security Analyst

N=160

		SA	A	NA	D	SD
As a result of my experiences in this course - Have a greater **appreciation for the need for prior planning**		101	44	12	2	1
As a result of my experiences in this course - I am **confident I can learn new skills** as needed for a cybersecurity work role		102	48	8	2	
As a result of my experiences in this course - I feel **more confident in my ability to secure work** in cybersecurity		71	67	11	10	1
As a result of my experiences in this course - I **feel more confident in my skills in cybersecurity**		62	65	24	5	3
As a result of my experiences in this course - I have a **better insight into what it will be like to work in cybersecurity**		99	43	11	3	3
As a result of my experiences in this course **- Improved my time management skills**		73	51	28	4	4

Common Question

Q&A

Links

- Work Role Definitions and Tasks
  - https://cyberindustry.org/Workrole
- NICCS Portal
  - https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool
- CSET Tool
  - https://cset-download.inl.gov/download
- Sugata Mitra Video
  - https://www.youtube.com/watch?v=dk60sYrU2RU&t=123s
- Kanban
  - www.mural.co
- Peer Review Paper
  - https://bmcmededuc.biomedcentral.com/articles/10.1186/s12909-021-02821-6
- Red Hat Academy
  - https://www.redhat.com/en/services/training/red-hat-academy
- Microsoft Software
  - https://portal.azure.com