

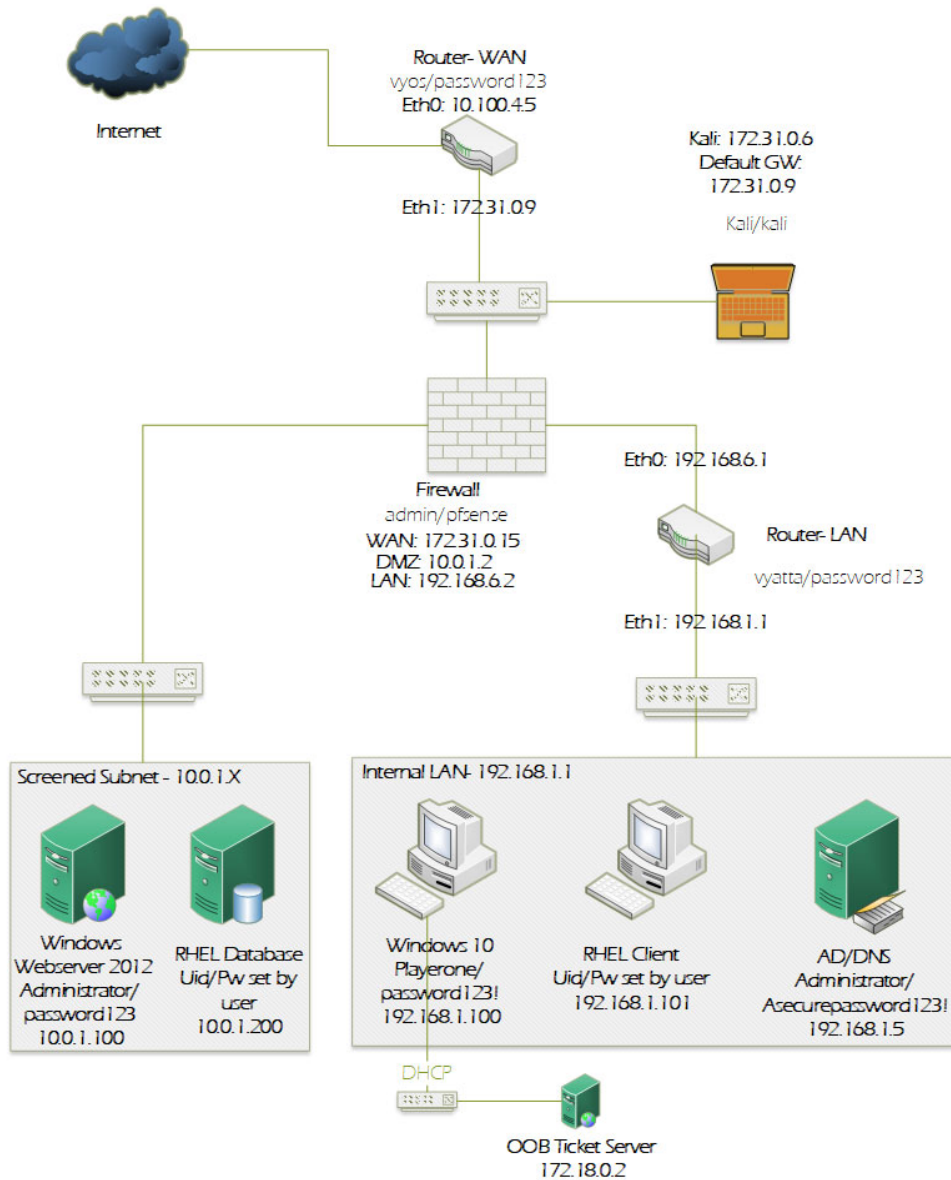
Welcome to the Cyber Career Challenge

The Cyber Career Challenge

- Is a “realistic” challenge for a team of students to demonstrate their competencies in cybersecurity work roles as well as to show their ability to problem solve and work as a team.

Work Role Interests

- NICE Framework and the Cybersecurity Work Roles
- Cyberindustry.org
- Work Role Interest Form
 - https://csusb.az1.qualtrics.com/jfe/form/SV_3sczDGAhEZwg46y
- Identify:
 - 3 work roles you are interested in
 - 3 tasks in each work role that you are most interested in



	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
AI		
	Use AI to develop a web app	Demo app
	Use local AI to assist with tasks	

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
	Device monitoring	Access information about device status
	Dashboard	dashboard displaying information
Backup and recovery solutions		
	Database is backup	Demonstrate backup
		Demonstrate restore
Change management		
	Change log	review change log
Vulnerability Assessment		
	Run a vulnerability scan	Review the scan report

AFRICAN PROVERB

*The best way to
eat an elephant
in your path is
to cut him up
into little pieces*

The best way to
solve a problem is
to tackle it bit by bit,
one step at a time.

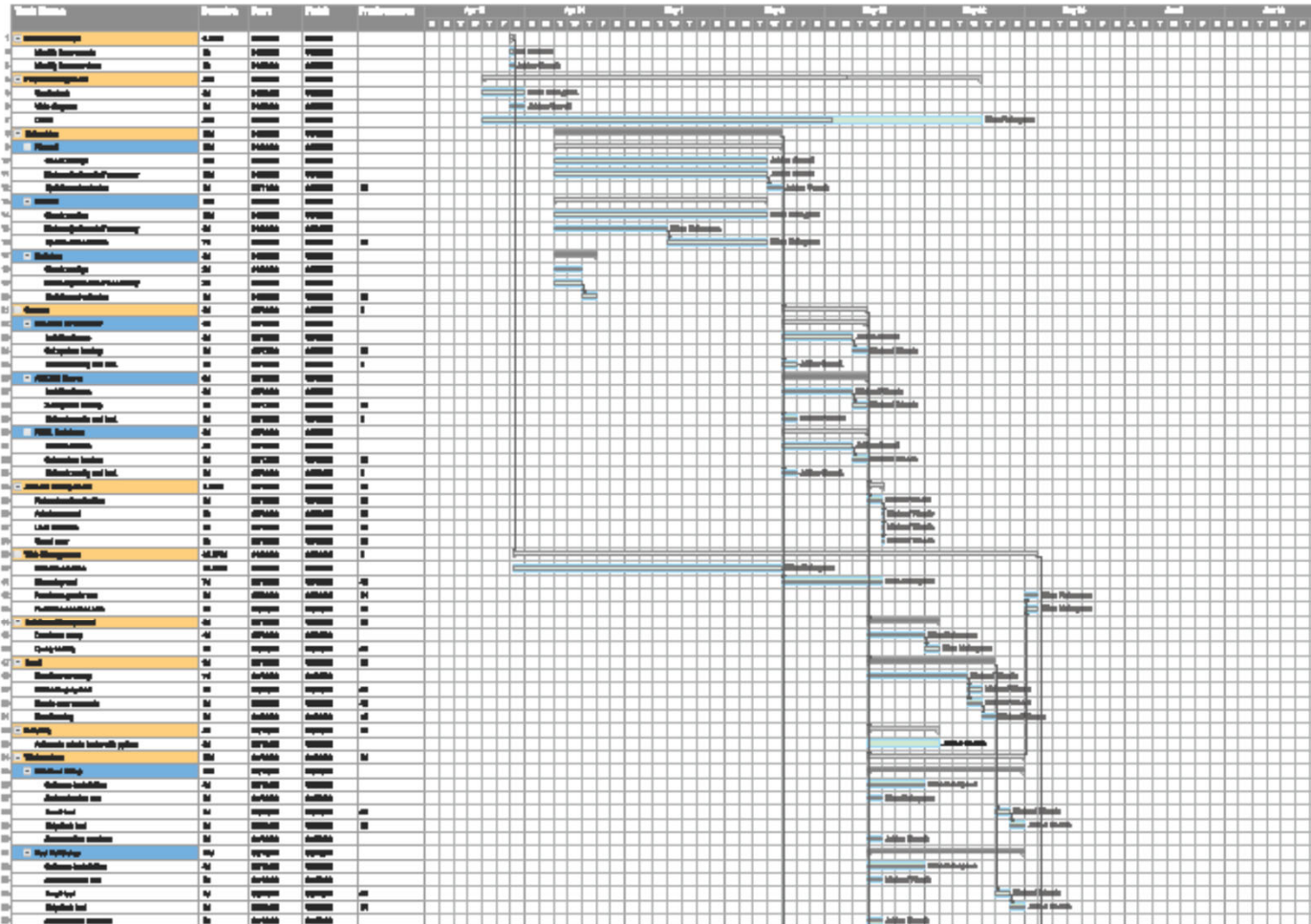


Presentations from prior year

Only a fool learns from his own mistakes. The wise man learns from the mistakes of others.

Otto von Bismarck

NCyTE Team 5 Project



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

Backlog

Inventory Network

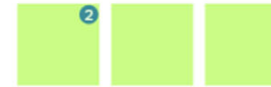
Build Basic Web Site

Build Database

Doing



Done



Determine Business Type



Team 1 Raptors [(Karen)] + [(Josh)] + [(Kyle)] + [(Darcel)]
<https://discord.gg/mex7bSh8F7>

Backlog

Doing

Rain Shrine	Rain Shrine	Rain Shrine
Present aion	Present aion	Present aion

Done

Project 1	Project 2	Project 3	Project 4	Project 5	Project 6	Project 7	Project 8	Project 9	Project 10	Project 11	Project 12	Project 13	Project 14	Project 15	Project 16	Project 17	Project 18	Project 19	Project 20	Project 21	Project 22	Project 23	Project 24	Project 25	Project 26	Project 27	Project 28	Project 29	Project 30
-----------	-----------	-----------	-----------	-----------	-----------	-----------	-----------	-----------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------

Team 1 Raptors [(Karen)] + [(Josh)] + [(Kyle)] + [(Darcel)]

What went well

What didn't go well

Actions

Team 3 - Scott/Shayne/Cameron/Silvia
<https://discord.gg/QWDQxm44>

Backlog

VISIO should be updated once we have access to our machines, and GANTT CHART should be adjusted according our workflow if it is necessary

Doing

Done

Project 1	Project 2	Project 3	Project 4	Project 5	Project 6	Project 7	Project 8	Project 9	Project 10	Project 11	Project 12	Project 13	Project 14	Project 15	Project 16	Project 17	Project 18	Project 19	Project 20	Project 21	Project 22	Project 23	Project 24	Project 25	Project 26	Project 27	Project 28	Project 29	Project 30
-----------	-----------	-----------	-----------	-----------	-----------	-----------	-----------	-----------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------

Team 3 -

What went well

What didn't go well

Actions

Team 5: "Urban Zen" Elton -- Ian -- Jaiden -- Michael

Backlog

Doing

Done

Project 1	Project 2	Project 3	Project 4	Project 5	Project 6	Project 7	Project 8	Project 9	Project 10	Project 11	Project 12	Project 13	Project 14	Project 15	Project 16	Project 17	Project 18	Project 19	Project 20	Project 21	Project 22	Project 23	Project 24	Project 25	Project 26	Project 27	Project 28	Project 29	Project 30
-----------	-----------	-----------	-----------	-----------	-----------	-----------	-----------	-----------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------	------------

Team 5

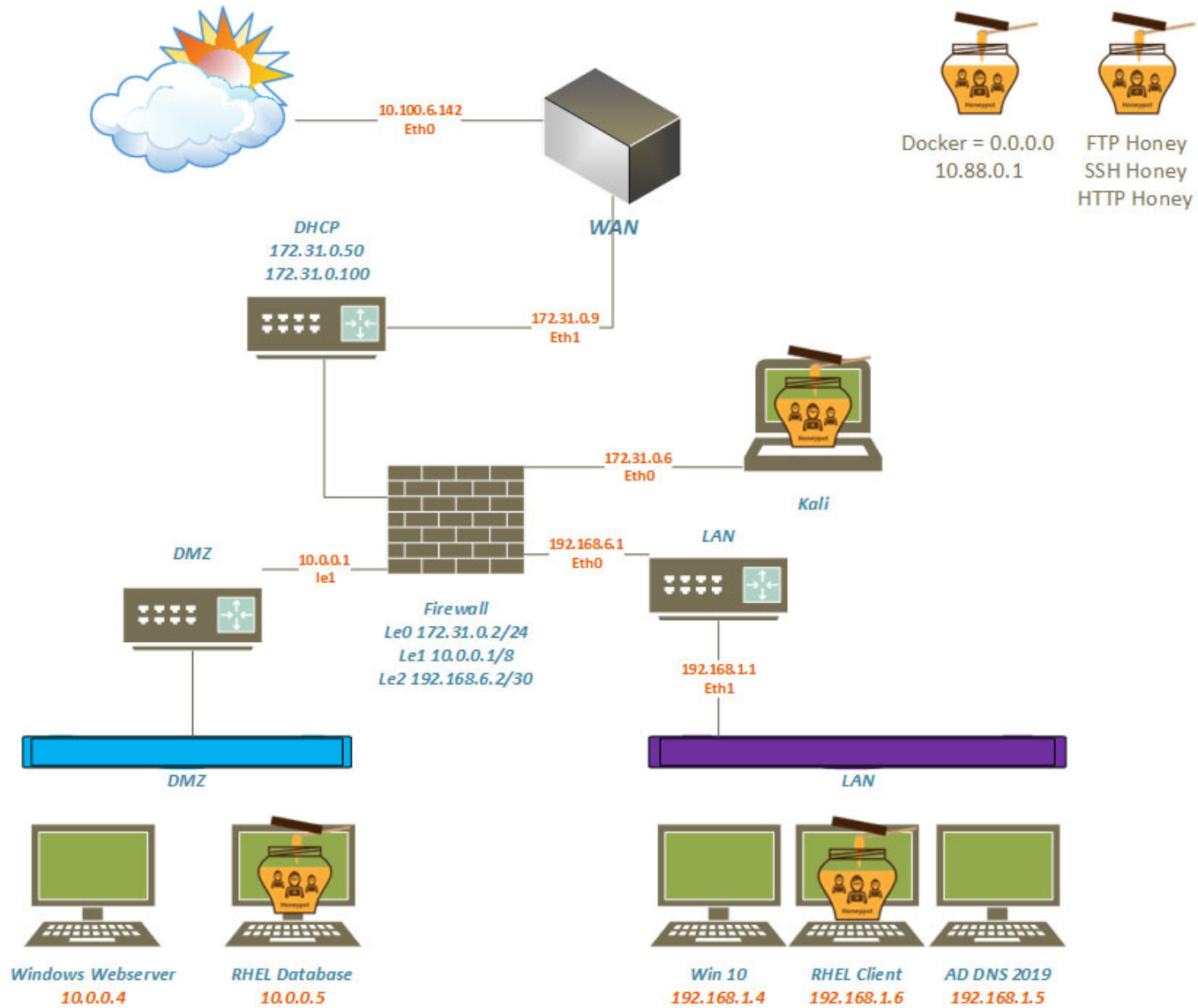
What went well

What didn't go well

Actions

Peer Review

- The student showed they were prepared during group meetings
- The student was punctual to meetings
- 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

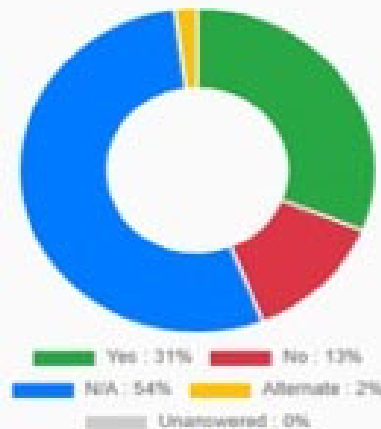


CSET

- NIST CSF: Framework for Improving Critical Infrastructure of Cybersecurity v1.1.
- Skipped many irrelevant questions, such as Temperature controls and Supply Chain Protections, but affected results.
 - Tried picking 'best' fit for assessing network

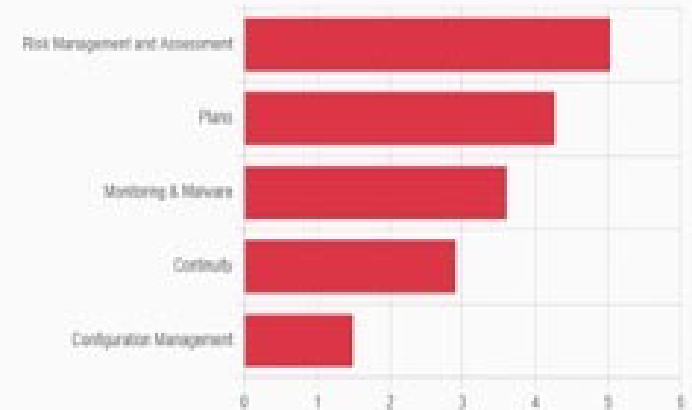
Standards Summary

This graph shows the overall answer percentages for each individual answer type.



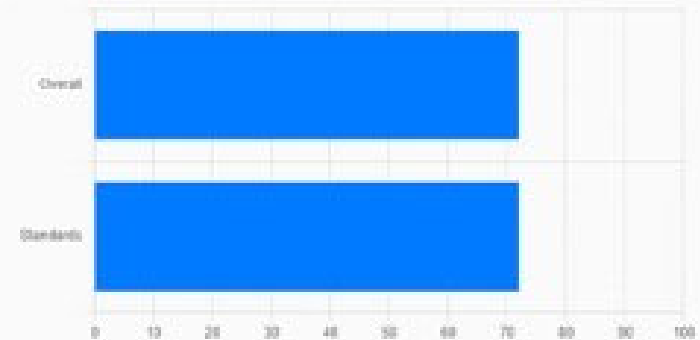
Top Ranked Categories

This graph shows the top areas of concern ranked. These are calculated from a weighted risk score based on the difficulty of attack. The attack weights are most heavily weighted for easy attacks to less for more difficult to attack.



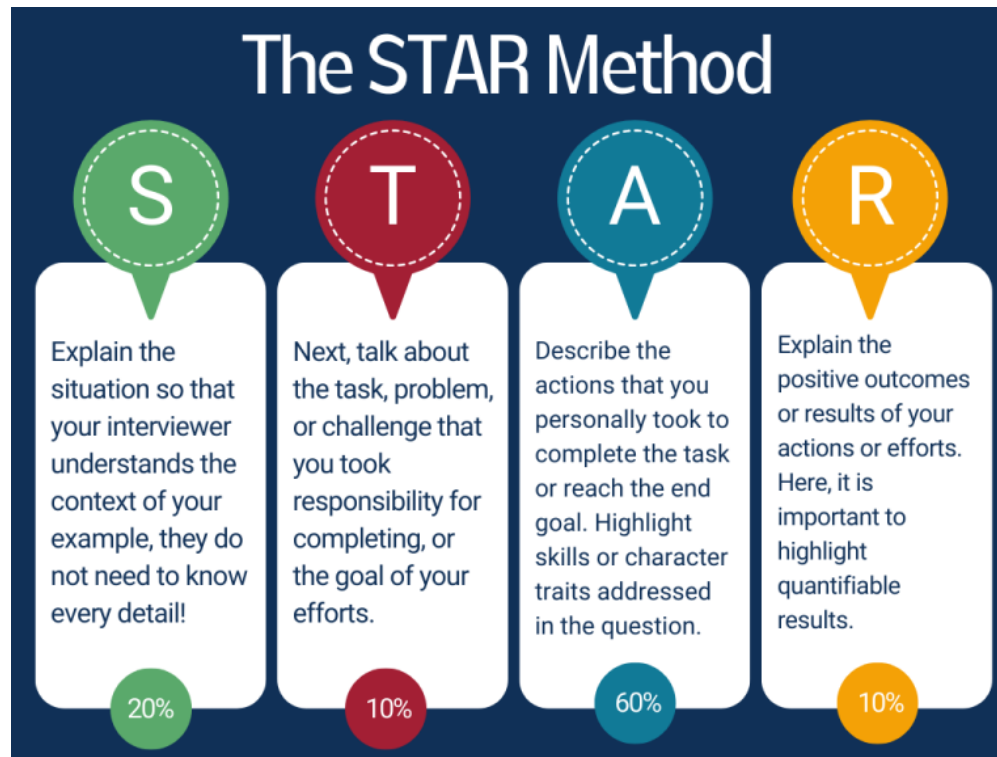
Assessment Compliance

This graph shows the overall percentage scores. Please note that unanswered questions are counted as a NO answer in these scores.



Red Team/Orange Team Week

The Star Method




CERTIFICATE

OF ACHIEVEMENT

CYBER CAREER CHALLENGE
2022


This certificate is proudly presented to

Your Name



Dr. Vincent Nestler
Cyber Career Challenge
Instructor

Corrinne Sande
NCyTE Director





The mission of the Cybersecurity Center at California State University, San Bernardino is to provide an exceptional education for the next generation of cybersecurity leaders for our region and our country. The Cybersecurity Center is the leader in developing applied and innovative education in cybersecurity that provides superior preparation for student success.

The National Cybersecurity Training and Education Center (NCYTE) at Watson Community College (WCC) is an Advanced Technological Education (ATE) National Center, grant-funded by the National Science Foundation (NSF). The National Cybersecurity Training & Education (NCYTE) Center advances professional development in the U.S. by investing in technological innovation, resources, and the workforce pipeline of tomorrow.

CERTIFICATE

OF ACHIEVEMENT

CYBER CAREER CHALLENGE 2022

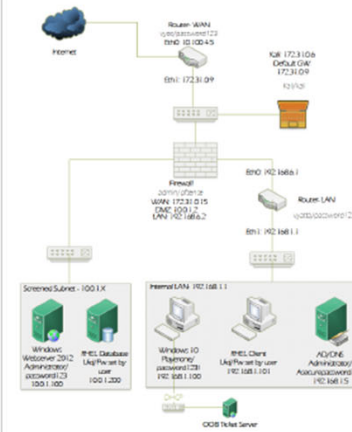
This certificate is proudly presented to

Your Name

Dr. Vincent Nestler
 Dr. Vincent Nestler
 Cyber Career Challenge
 Instructor

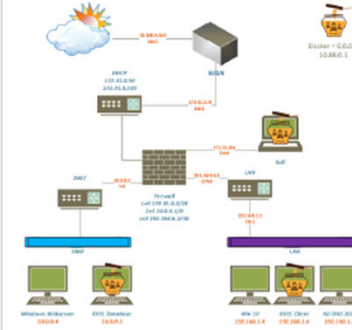
Corrinne Sande
 NCYTE Director

The Cyber Career Challenge 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 identified
	Identified three services	List of items identified
Project Management	Gantt Chart	Completed Chart Posted
	Visio diagram of network	Diagram is accurate - information is correct
	Facilities System Security Plan	Accurate and complete
Account Management	Network configuration	Access the network admin console
	Admin account	Log in as user
	User accounts	Log in as user
	Guest user account (such as contractor)	Log in as a guest user
Web Management	Web site created	Access website from browser
	Shipping cart	access shipping cart on website
	purchase goods	purchase a good
	purchase service	purchase a service
Database Management	Database setup	Access database interface
	Query data in 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
Set up Active Directory w/ Server Manager	Configure, implement, configure, and support of system components	System Administrator
Created a server and proxied to Server Controller	Install, update, and troubleshoot systems/services	System Administrator
Configured DC with a single forest	Monitor and maintain systems/service configuration	System Administrator
Created email accounts for users	Manage accounts, network rights, and access to systems and equipment	System Administrator
Established database to certain events	Install, update, and troubleshoot systems/services	System Administrator
Setup Thunderbird as email client to user GUI	Check system hardware availability, functionality, integrity, and efficiency	System Administrator

Used binary path in Bash to help find and locate binaries	Identify and/or develop secure engineering tasks to enhance capabilities and detect vulnerabilities	System Administrator / Cyber Threat Intelligence Analyst
Help to configure OpenVPN for setup	Configure and optimize network links, routes, and protocols (e.g., higher-level protocols, tunneling)	Network Operations Specialist
Created Group Policy Objects	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs	Network Operations Specialist
Disabled all unnecessary services on Windows Machines	Adapt and integrate security controls based on principles of least privilege and need-to-know	Cyber Defense Analyst
Used nmap to configure security settings automatically	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity	Cyber Defense Analyst
Implemented live team scripts for Windows	Perform security reviews and identify security gaps to security architecture leading to recommendations for inclusion in the risk mitigation strategy	Cyber Defense Analyst
Conducted audits after Windows scripts	Assess and monitor system security related to system implementation and testing practices	Cyber Defense Analyst
Run daily windows virus scans	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity	Cyber Defense Analyst
Reduced size config and advanced console windows presentation logs	Analyze identified malicious activity to determine weaknesses, exploit, exploitation methods, effects on system and information	Cyber Defense Analyst
Applied network traffic with Wireshark	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools	Cyber Defense Analyst
Scanned malware on Windows and found all ability of source	Isolate and remove malware	Cyber Defense Analyst
Reproduced live malware and set up Wireshark to identify possible active diffms and files	Reconstruct a malicious attack or activity based off network traffic	Cyber Defense Analyst
Installed control program (GPO) for users	Apply security-related security architecture principles to meet organizational confidentiality, integrity and availability requirements	System Security Analyst
Applied GPOs to give security defense against user machines being used to attack system	Apply security policies to applications that interface with user interfaces, such as Business for Business (B2B) applications	System Security Analyst

Testimonials

- “... at my job interview I explained what I did during the capstone. They hired me the next morning.”
- “... this really gave me the confidence I needed at my job interview. I did not feel like a poser.”

Who should apply and how to be successful

- Students toward the end of their course of study
- Students with time
- Self motivated and highly engaged
- Similar to a long form CCDC
- Professor/mentor
- Timezone
- Balanced skillset