FDU

Personal. Global. Transformational.

Program of Study Validation: Cybersecurity Concentration at FDU

DEPARTMENT OF
MATH & COMPUTER SCIENCE

IHAB DARWISH, PHD

DIRECTOR OF CYBERSECURITY
PROGRAM – FLORHAM CAMPUS

Fairleigh Dickinson University

FDU is ranked among the "**Best Regional Universities"**

U.S. News & World Report

#44 in the North region

U.S. News & World Report

Ranked among "America's Best Colleges"

Forbes magazine

Listed among the "Top U.S. colleges"

Wall Street Journal/Times Higher Education rankings

Number 21 in "Best Value Schools"

U.S. News & World Report

Cybersecurity on Demand

- High demand for cyber security professionals and is expected to grow even more in the coming years, in the public and the private sectors.
- Employment rate in the field of cyber security is projected to grow 33% by 2030 *(U.S. Bureau of Labor Statistics)*.
- There will be 3.5 million unfilled cybersecurity jobs globally by 2025, up from one million positions in 2014 *(New York Times & Cybersecurity Ventures)*.
- Cyber security professionals are needed to protect computer networks and systems in the financial, communication, energy and transportation industries as well as in the government, against cyber-attacks.

Computer Science Programs at FDU - Florham

- BS in Computer Science
- **BS in Computer Science - concentrations**
  - Game Development
  - **Cybersecurity – Validated Program**
  - Data Science
- Combined BS/MS in Computer Science – a 5 Year Program!
  - Requirements (application in Sophomore or Junior year): completion of 15 credits of CS courses (5 courses) and maintaining a major GPA of at least 3.0

Cybersecurity At FDU

- Cutting edge courses developed in accordance with the curricular guidelines of the NSA *(National Security Agency)* and DoD *(Department of Defense)*.

- Our program enables students to become certified (Security+, Network+, CISSP and CCNA).

- Our graduates land positions in both the private and the public sectors.

Center for Cyber Security and Information Assurance

- Fairleigh Dickinson University is a National Center of Academic Excellence in Information Assurance Education (CAE/CDE) since 2013
- On April 25, 2022, Fairleigh Dickinson University was Awarded National Center of Academic Excellence in Cyber Defense (CAE-CD) Designation certificate .
- Center for Cyber Security and Information Assurance at FDU
  - academic programs in cyber security meet the demands of industry and the government.
  - academic and research opportunists for students.

Center for Cyber Security and Information Assurance

- The redesignation process involved first the validation of the Bachelor of Science in Computer Science **(BSCS) with Cybersecurity concentration program of study (POS)** offered by the Department of Mathematics and Computer Science, Becton College, Florham Campus. Dr. Darwish as the Point of Contact (POC) successfully led the effort towards getting the BSCS with Cybersecurity concentration POS validated.
- Following the POS validation, Dr. Mondal as FDU’s Point of Contact (POC) for the NCAE-C led efforts towards obtaining the current designation valid till the academic year 2026.

Program of Study (PoS) Validation

- Programs of Study (PoS) is defined as set of courses that are designed to develop program outcomes in the student population over time.
- PoS validation will lead to CAE designation
- For PoS validation:
  - The institution must show its curriculum path
  - Provide evidence that students are enrolled in the path, successfully complete the path and receive recognition for completing the path.
  - All institutions applying for PoS validation must be regionally accredited. FDU is accredited by the Middle States Commission on Higher Education and licensed by the State of New Jersey Commission on Higher Education

FDU PoS Validation Project Timeline

Planning Stage – 2019 - 2020

Submission Date for Pre-review Dec 15, 2020

Feedback Submitted Dec 28th, 2020

Final Application Submitted January 15th, 2021

Submitted for NSA Final Review July 30, 2021

Application Approved August 19, 2021

- ❖ Planning Stage Jan 2019 – Dec 2020
- ❖ Pre-Submission Review – Dec 15th, 2020
- ❖ Feedback Submission – Dec 28th, 2020
- ❖ Final Application Submitted – Jan15th, 2021
- ❖ Submitted for Peer Review Committee – June 2021
- ❖ Submitted to NSA Final Review July 30th, 2021
- ❖ Application Approved August 19th, 2021

Program of Study (PoS) Validation Planning Activities – 4 Domains

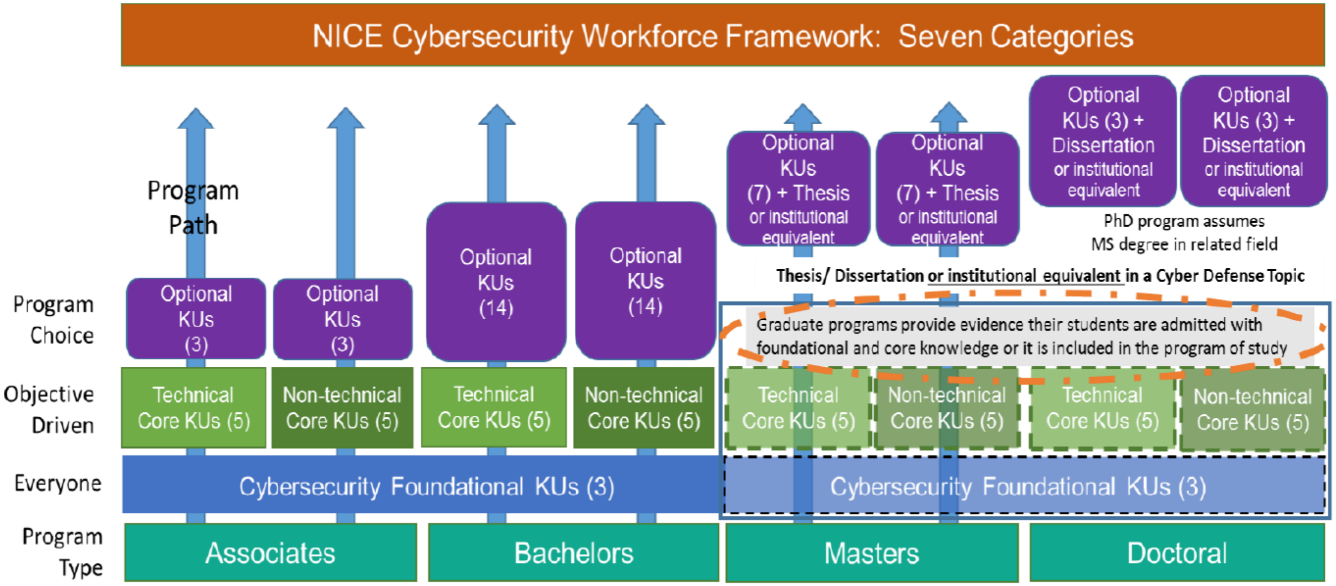
1. **PoS Curriculum**
2. Students
3. Faculty Members
4. **Continuous Improvement**

1. PoS Curriculum

- As part of the continuous improvement process for our BS Computer Science degree with Cybersecurity Concentration Program of Study (PoS), we have been periodically preparing and implementing several action plans to enhance our program.
- Throughout the designation cycle from 2015 to 2020, we have encountered and resolved several shortfalls in our program and implemented Curricular changes for AYs 2015-2020.

1. PoS Curriculum

In 2019, CAE-CDE introduced a new set of Knowledge Units (KUs) with new alignment requirements. Bachelors Programs now align to 22 KUs (3 Foundational, 5 Technical/ Non-Technical in addition to 14 KUs (Selected from the Optional Li



NICE Cybersecurity Workforce Framework: Seven Categories

Program Path

Program Choice

Objective Driven

Everyone

Program Type

Optional KUs (3)

Optional KUs (3)

Optional KUs (14)

Optional KUs (14)

Optional KUs (7) + Thesis or institutional equivalent

Optional KUs (7) + Thesis or institutional equivalent

Optional KUs (3) + Dissertation or institutional equivalent

Optional KUs (3) + Dissertation or institutional equivalent

PhD program assumes MS degree in related field

Thesis/ Dissertation or institutional equivalent in a Cyber Defense Topic

Graduate programs provide evidence their students are admitted with foundational and core knowledge or it is included in the program of study

Technical Core KUs (5)

Non-technical Core KUs (5)

Technical Core KUs (5)

Non-technical Core KUs (5)

Technical Core KUs (5)

Non-technical Core KUs (5)

Technical Core KUs (5)

Non-technical Core KUs (5)

Cybersecurity Foundational KUs (3)

Cybersecurity Foundational KUs (3)

Associates

Bachelors

Masters

Doctoral

https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2020_Knowledge_Units.pdf

1. PoS Curriculum

- 1a. The cybersecurity PoS offered by the institution
- 1b. NICE Framework crosswalk alignment
- 1c. Courses Syllabi and Courses Requiring Applied Lab Exercises (For KU Aligned Courses Only)
- 1d. Curriculum Map and Assessment Documentation
- 1e. KU alignment

1a. The cybersecurity PoS offered by the institution

POS:BSCS with Cybersecurity Concentration

- **BS Computer Science degree with Cybersecurity Concentration -Dr. Laila Khreisat, Department Chair**
- **Was initially introduced in 2012 and designated in 2015**
- https://www.fdu.edu/program/bs-computer-science-florham/
- PoS Curriculum Map and Plan + KU Aligned Courses
  - 48 Credits (16 Courses) are required in the program
  - 18 Credits are required for the Cybersecurity Concentration
  - 10 Courses are currently KUs Aligned
  - In Fall 2020, we have introduced two new cybersecurity courses with new alignment to the KUs

Becton College of Arts and Sciences
Department of Math & Computer Science

Bachelor of Science in Computer Science
Cybersecurity Concentration

Required Major Courses (30 Credits)	Required Cybersecurity Concentration Cources (18 Credits)
CSCI 1205 Introduction to Computer Programming (3) – C#	CSCI 3157 Cybersecurity (3)
CSCI 2215 Introduction to Computer Science (3) – C++	CSCI 3666 Data Communication and Computer Networks (3)
CSCI 2216 Introduction to Computer Science II (3)	CSCI 3158 Information Security Design and Mgm't (3)
CSCI 2255 Discrete Structures (3)	CSCI 3355 Intro to Cryptography (3)
CSCI 2233 Data Structures & Algorithms (3)	CSCI 3869 Network Security (3)
CSCI 3371 Computer Modeling & Simulation (3) or MATH 3300 Statistics (3)	CSCI 3870 Security Regulations, Detection & Forensics (3)
CSCI 3278 Operating Systems (3)	
CSCI 3315 Software Design (3)	
CSCI 3304 Computer Organizations (3)	
CSCI 4498 Internship (3)	

Courses in green cells are the newly aligned courses with KU

1b. NICE Framework crosswalk alignment

Securely Provision (SP)

Operate and Maintain (OM)

Oversee and Govern (OV)

Protect and Defend (PR)

Analyze (AN)

Collect and Operate (CO)

Investigate (IN)

Our program is geared to enhance the knowledge set to learn how to protect systems, with defense strategies and capabilities and to learn advanced techniques on how to analyze systems, infrastructures and data captured throughout the process

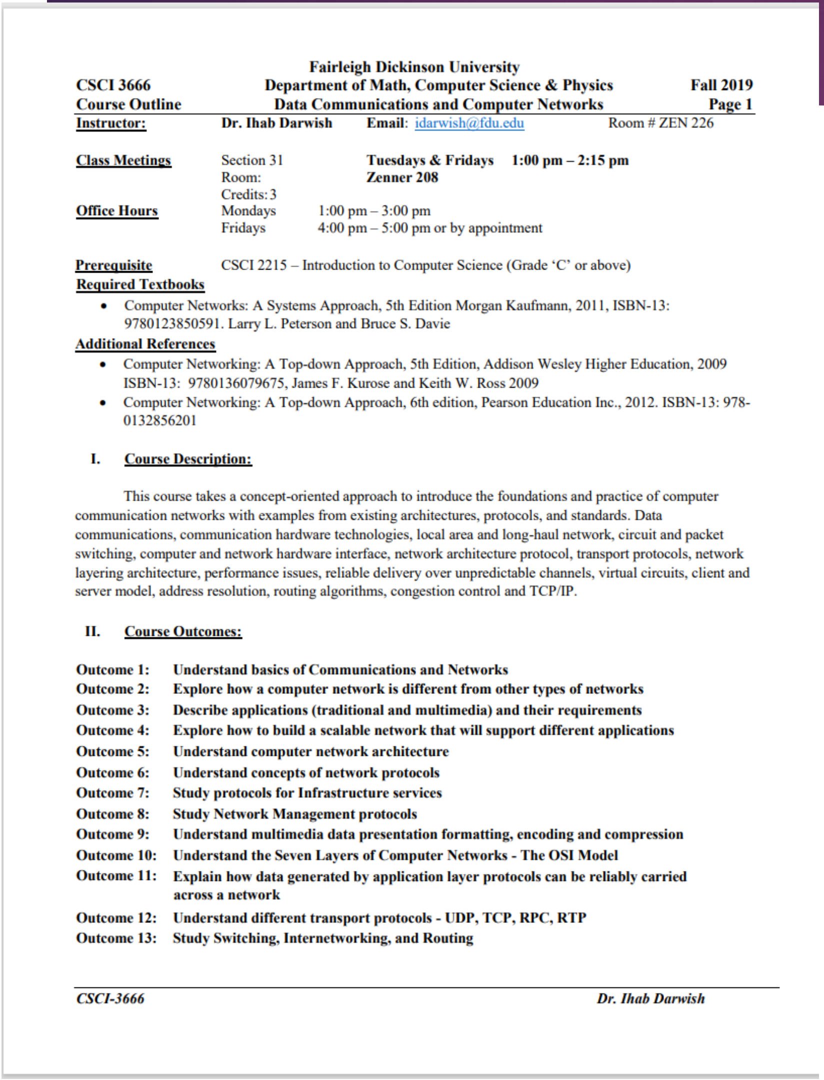
- Workforce Framework for Cybersecurity (NICE Framework) (nist.gov)

1c. Courses Syllabi and Courses Requiring Applied Lab Exercises (For KU Aligned Courses Only)

- **CSCI1205 Intro to Computer Programming**
- **CSCI2215 Intro to Computer Science**
- **CSCI2233 Data Structures & Algorithms**
- **CSCI3157 Cybersecurity**
- **CSCI3666 Data Comm & Computer Networks**
- **CSCI3869 Network Security**

- In our program, we have provided 10 courses that are aligned with KUs and selected only six courses that require applied lab Exercises
- Samples of course outlines and the Lab Exercises are provided

Course Outlines Samples



Fairleigh Dickinson University

CSCI 3666 — **Department of Math, Computer Science & Physics** — **Fall 2019**

Course Outline — **Data Communications and Computer Networks** — **Page 1**

Instructor: **Dr. Ihab Darwish** **Email:** idarwish@fdu.edu Room # ZEN 226

Class Meetings Section 31 **Tuesdays & Fridays 1:00 pm – 2:15 pm**
Room: **Zenner 208**
Credits: 3

Office Hours Mondays 1:00 pm – 3:00 pm
Fridays 4:00 pm – 5:00 pm or by appointment

Prerequisite CSCI 2215 – Introduction to Computer Science (Grade 'C' or above)

Required Textbooks

- Computer Networks: A Systems Approach, 5th Edition Morgan Kaufmann, 2011, ISBN-13: 9780123850591. Larry L. Peterson and Bruce S. Davie

Additional References

- Computer Networking: A Top-down Approach, 5th Edition, Addison Wesley Higher Education, 2009 ISBN-13: 9780136079675, James F. Kurose and Keith W. Ross 2009
- Computer Networking: A Top-down Approach, 6th edition, Pearson Education Inc., 2012. ISBN-13: 978-0132856201

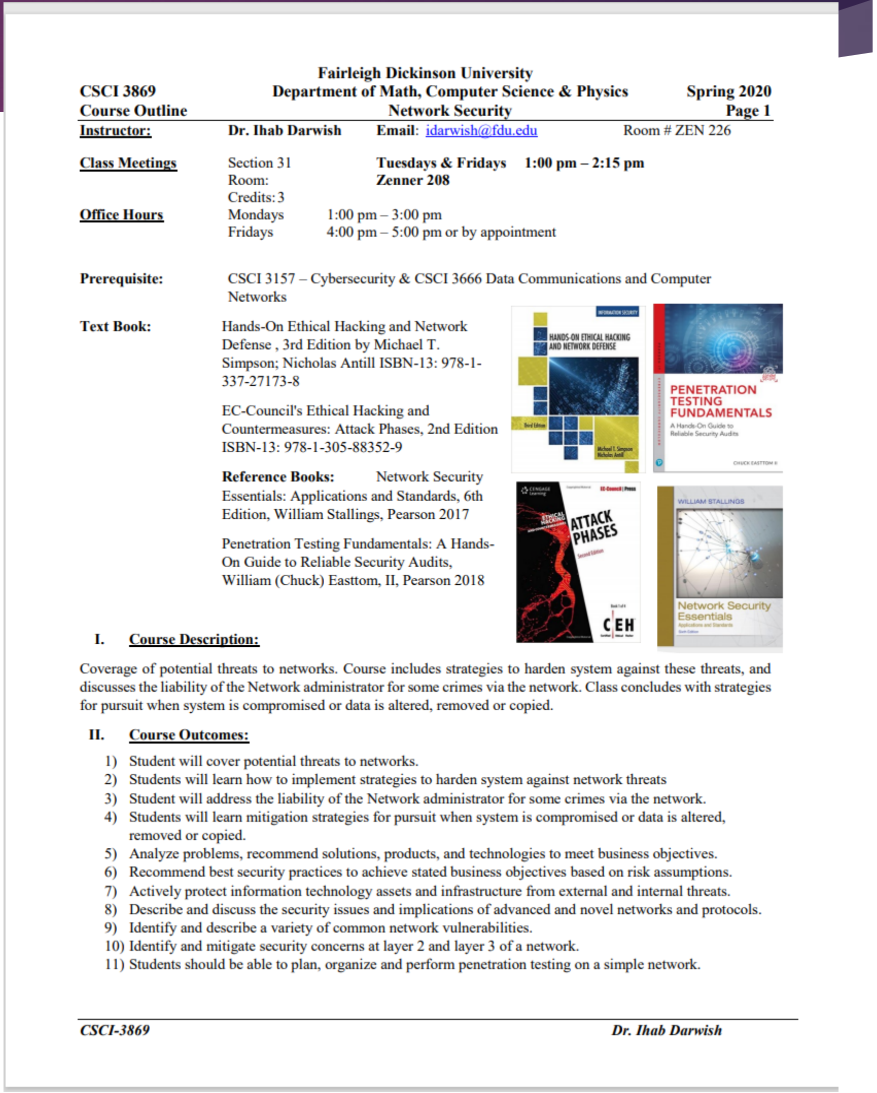
I. Course Description:

This course takes a concept-oriented approach to introduce the foundations and practice of computer communication networks with examples from existing architectures, protocols, and standards. Data communications, communication hardware technologies, local area and long-haul network, circuit and packet switching, computer and network hardware interface, network architecture protocol, transport protocols, network layering architecture, performance issues, reliable delivery over unpredictable channels, virtual circuits, client and server model, address resolution, routing algorithms, congestion control and TCP/IP.

II. Course Outcomes:

Outcome 1: Understand basics of Communications and Networks
Outcome 2: Explore how a computer network is different from other types of networks
Outcome 3: Describe applications (traditional and multimedia) and their requirements
Outcome 4: Explore how to build a scalable network that will support different applications
Outcome 5: Understand computer network architecture
Outcome 6: Understand concepts of network protocols
Outcome 7: Study protocols for Infrastructure services
Outcome 8: Study Network Management protocols
Outcome 9: Understand multimedia data presentation formatting, encoding and compression
Outcome 10: Understand the Seven Layers of Computer Networks - The OSI Model
Outcome 11: Explain how data generated by application layer protocols can be reliably carried across a network
Outcome 12: Understand different transport protocols - UDP, TCP, RPC, RTP
Outcome 13: Study Switching, Internetworking, and Routing

CSCI-3666 *Dr. Ihab Darwish*



Fairleigh Dickinson University

CSCI 3869 — **Department of Math, Computer Science & Physics** — **Spring 2020**

Course Outline — **Network Security** — **Page 1**

Instructor: **Dr. Ihab Darwish** **Email:** idarwish@fdu.edu Room # ZEN 226

Class Meetings Section 31 **Tuesdays & Fridays 1:00 pm – 2:15 pm**
Room: **Zenner 208**
Credits: 3

Office Hours Mondays 1:00 pm – 3:00 pm
Fridays 4:00 pm – 5:00 pm or by appointment

Prerequisite: CSCI 3157 – Cybersecurity & CSCI 3666 Data Communications and Computer Networks

Text Book: Hands-On Ethical Hacking and Network Defense , 3rd Edition by Michael T. Simpson; Nicholas Antill ISBN-13: 978-1-337-27173-8

EC-Council's Ethical Hacking and Countermeasures: Attack Phases, 2nd Edition ISBN-13: 978-1-305-88352-9

Reference Books: Network Security Essentials: Applications and Standards, 6th Edition, William Stallings, Pearson 2017

Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits, William (Chuck) Easttom, II, Pearson 2018

HANDS-ON ETHICAL HACKING AND NETWORK DEFENSE
PENETRATION TESTING FUNDAMENTALS
A Hands-On Guide to Reliable Security Audits
ATTACK PHASES
CEH
WILLIAM STALLINGS
Network Security Essentials

I. Course Description:

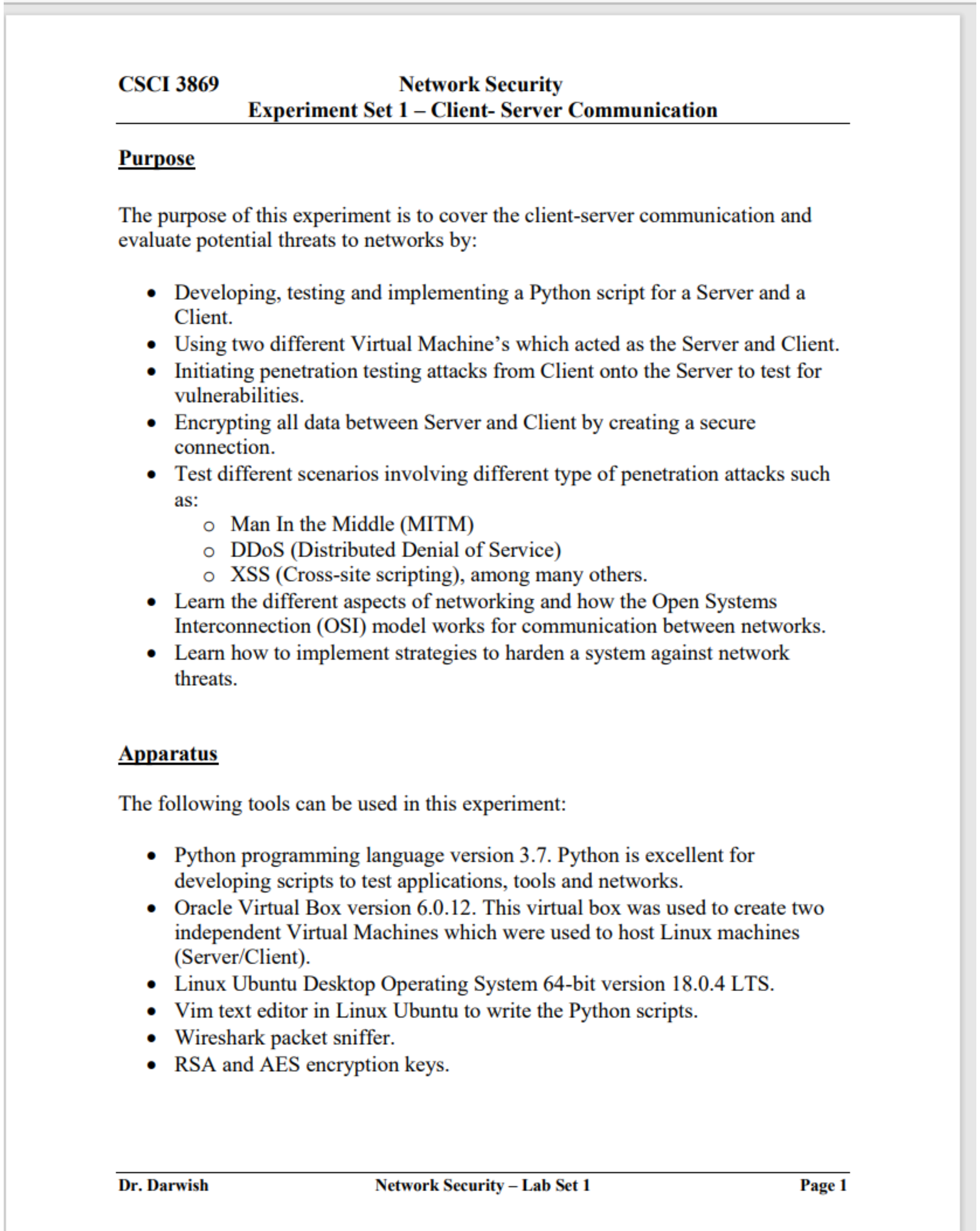
Coverage of potential threats to networks. Course includes strategies to harden system against these threats, and discusses the liability of the Network administrator for some crimes via the network. Class concludes with strategies for pursuit when system is compromised or data is altered, removed or copied.

II. Course Outcomes:

1) Student will cover potential threats to networks.
2) Students will learn how to implement strategies to harden system against network threats
3) Student will address the liability of the Network administrator for some crimes via the network.
4) Students will learn mitigation strategies for pursuit when system is compromised or data is altered, removed or copied.
5) Analyze problems, recommend solutions, products, and technologies to meet business objectives.
6) Recommend best security practices to achieve stated business objectives based on risk assumptions.
7) Actively protect information technology assets and infrastructure from external and internal threats.
8) Describe and discuss the security issues and implications of advanced and novel networks and protocols.
9) Identify and describe a variety of common network vulnerabilities.
10) Identify and mitigate security concerns at layer 2 and layer 3 of a network.
11) Students should be able to plan, organize and perform penetration testing on a simple network.

CSCI-3869 *Dr. Ihab Darwish*

Lab Exercises Samples



CSCI 3869 Network Security
Experiment Set 1 – Client- Server Communication

Purpose

The purpose of this experiment is to cover the client-server communication and evaluate potential threats to networks by:

- Developing, testing and implementing a Python script for a Server and a Client.
- Using two different Virtual Machine's which acted as the Server and Client.
- Initiating penetration testing attacks from Client onto the Server to test for vulnerabilities.
- Encrypting all data between Server and Client by creating a secure connection.
- Test different scenarios involving different type of penetration attacks such as:
  - Man In the Middle (MITM)
  - DDoS (Distributed Denial of Service)
  - XSS (Cross-site scripting), among many others.
- Learn the different aspects of networking and how the Open Systems Interconnection (OSI) model works for communication between networks.
- Learn how to implement strategies to harden a system against network threats.

Apparatus

The following tools can be used in this experiment:

- Python programming language version 3.7. Python is excellent for developing scripts to test applications, tools and networks.
- Oracle Virtual Box version 6.0.12. This virtual box was used to create two independent Virtual Machines which were used to host Linux machines (Server/Client).
- Linux Ubuntu Desktop Operating System 64-bit version 18.0.4 LTS.
- Vim text editor in Linux Ubuntu to write the Python scripts.
- Wireshark packet sniffer.
- RSA and AES encryption keys.

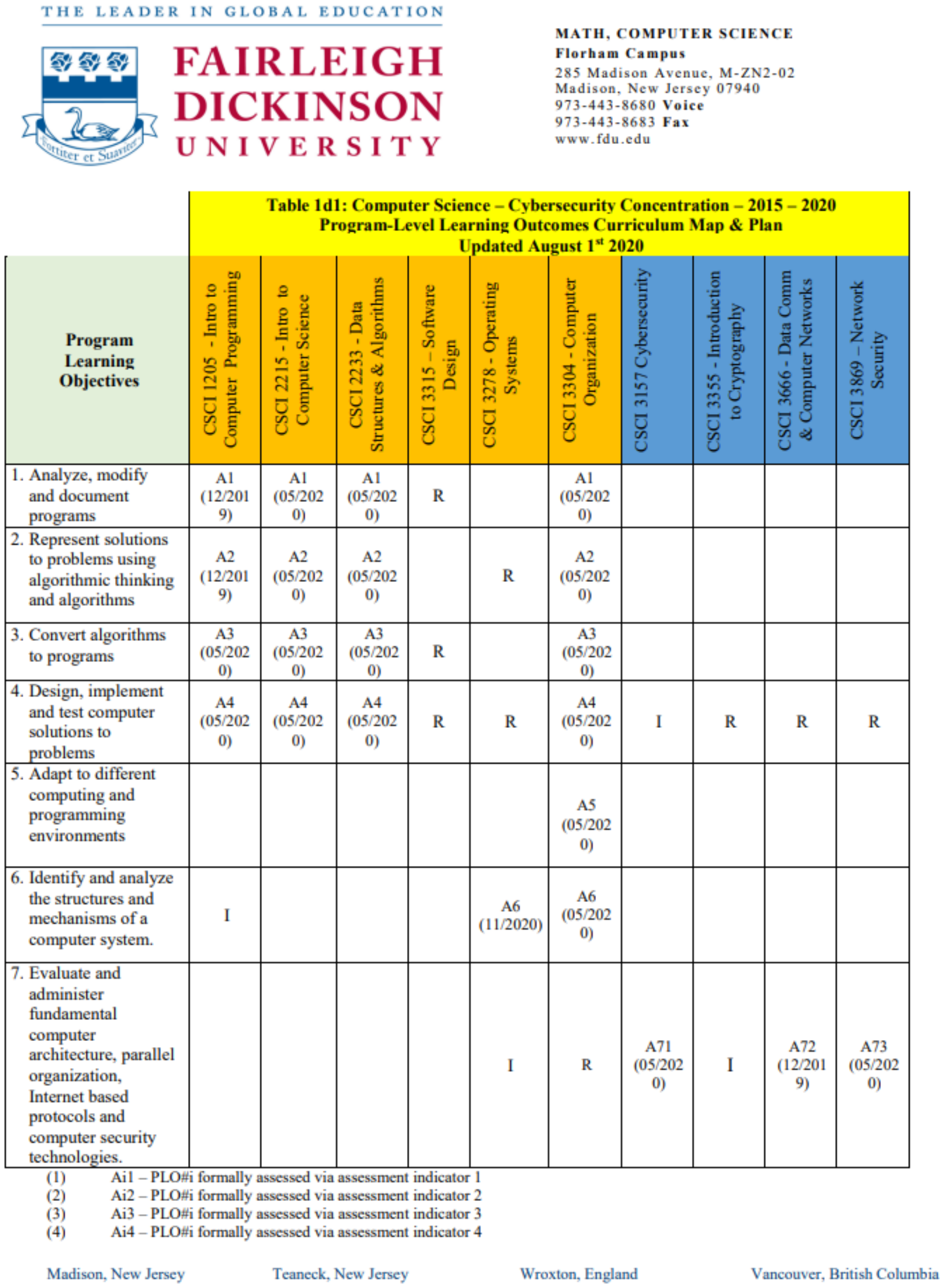
Dr. Darwish **Network Security – Lab Set 1** **Page 1**

1d. Curriculum Map and Plan with Assessment Documentation

- **State the Program-Level Learning Outcomes of the PoS, provide documentation of the Program-Level Learning Outcomes**
- **Provide evidence for the Program-Level Learning Outcomes Curriculum Map and Plan that identified the PoS courses where the outcomes are assessed**
- **Provide documentation for the General Information for each Program-Level Learning Outcome**
- **Provide documentation for the Assessment of Indicators for each Program-Level Learning Outcome**
- **Provide documentation for the Overall Assessment Information of each Program-Level Learning Outcome**

1d. Program-Level Learning Outcomes of the PoS

1. Analyze, modify and document programs
2. Represent solutions to problems using algorithmic thinking and algorithms
3. Convert algorithms to programs
4. Design, implement and test computer solutions to problems
5. Adapt to different computing and programming environments
6. Identify and analyze the structures and mechanisms of a computer system.
7. Evaluate and administer fundamental computer architecture, parallel organization, Internet based protocols and computer security technologies.



THE LEADER IN GLOBAL EDUCATION

FAIRLEIGH DICKINSON UNIVERSITY

Fortiter et Suaviter

MATH, COMPUTER SCIENCE
Florham Campus
285 Madison Avenue, M-ZN2-02
Madison, New Jersey 07940
973-443-8680 Voice
973-443-8683 Fax
www.fdu.edu

Table 1d1: Computer Science – Cybersecurity Concentration – 2015 – 2020
Program-Level Learning Outcomes Curriculum Map & Plan
Updated August 1st 2020

Program Learning Objectives	CSCI 1205 - Intro to Computer Programming	CSCI 2215 - Intro to Computer Science	CSCI 2233 - Data Structures & Algorithms	CSCI 3315 – Software Design	CSCI 3278 - Operating Systems	CSCI 3304 - Computer Organization	CSCI 3157 Cybersecurity	CSCI 3355 - Introduction to Cryptography	CSCI 3666 - Data Comm & Computer Networks	CSCI 3869 – Network Security
1. Analyze, modify and document programs	A1 (12/2019)	A1 (05/2020)	A1 (05/2020)	R		A1 (05/2020)				
2. Represent solutions to problems using algorithmic thinking and algorithms	A2 (12/2019)	A2 (05/2020)	A2 (05/2020)		R	A2 (05/2020)				
3. Convert algorithms to programs	A3 (05/2020)	A3 (05/2020)	A3 (05/2020)	R		A3 (05/2020)				
4. Design, implement and test computer solutions to problems	A4 (05/2020)	A4 (05/2020)	A4 (05/2020)	R	R	A4 (05/2020)	I	R	R	R
5. Adapt to different computing and programming environments						A5 (05/2020)				
6. Identify and analyze the structures and mechanisms of a computer system.	I				A6 (11/2020)	A6 (05/2020)				
7. Evaluate and administer fundamental computer architecture, parallel organization, Internet based protocols and computer security technologies.					I	R	A71 (05/2020)	I	A72 (12/2019)	A73 (05/2020)

(1) Ai1 – PLO#i formally assessed via assessment indicator 1
(2) Ai2 – PLO#i formally assessed via assessment indicator 2
(3) Ai3 – PLO#i formally assessed via assessment indicator 3
(4) Ai4 – PLO#i formally assessed via assessment indicator 4

Madison, New Jersey Teaneck, New Jersey Wroxton, England Vancouver, British Columbia

1d. Program-Level Learning Outcomes Curriculum Map and Plan

1d. General information for each Program-Level learning outcome (PLO1 – PLO7)

Table 1: General Information for PLO 1

Date report submitted	05-31-2020
Program faculty who contributed to this report	Laila Khreisat, Neelu Sinha, Kiron Sharma, Gurjot Singh, Ihab Darwish
Program-level Learning Outcome	Analyze, modify and document programs
Course(s) that formally assess(es) this program-level learning outcome (at its highest level, see curriculum map, Table 1d.1)	CSCI 1205 - Intro to Computer Programming CSCI 2215 - Intro to Computer Science CSCI 2233 - Data Structures & Algorithms CSCI3304 - Computer Organization
Number of students assessed for this program-learning level outcome	CSCI 1205-18 CSCI 2215-16 CSCI 2233-9 CSCI 3304-8
Quarter/semester students were assessed.	Fall 2019 (CSCI 1205), Spring 2020 CSCI 2215, 2233, 3304

1d. Assessment of Indicators for each Program-Level Learning Outcome

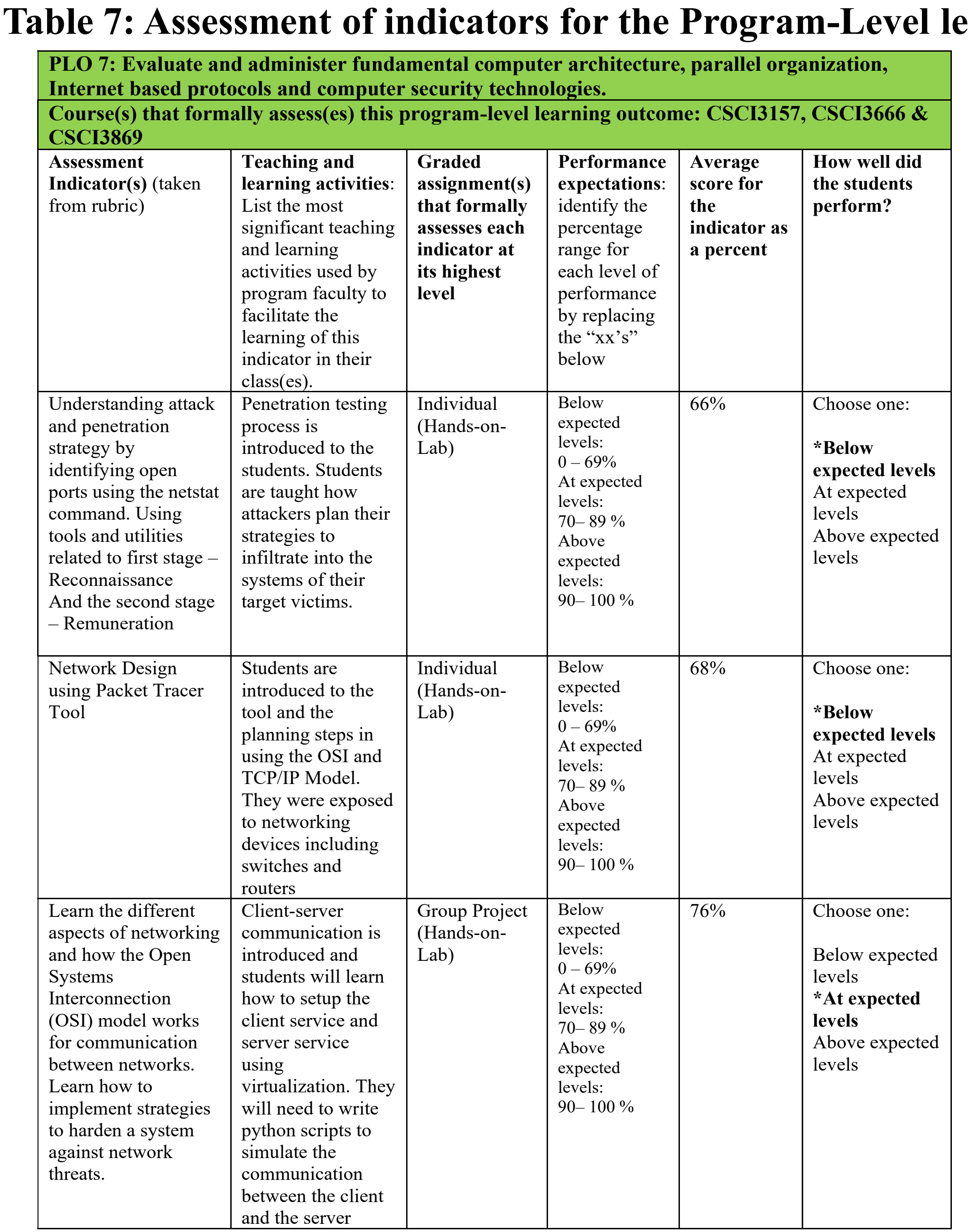
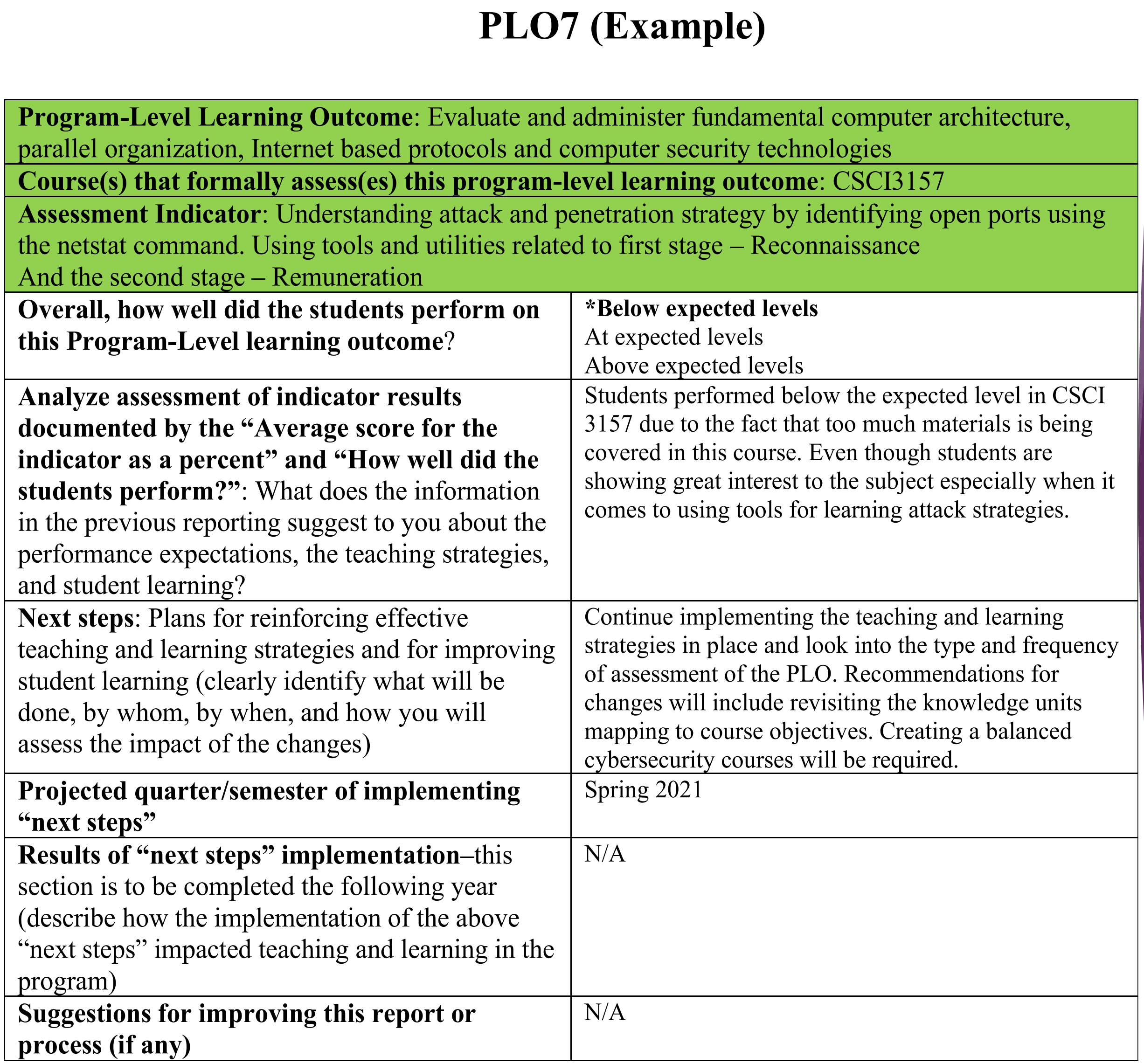


Table 7: Assessment of indicators for the Program-Level learning outcome 7

PLO 7: Evaluate and administer fundamental computer architecture, parallel organization, Internet based protocols and computer security technologies.					
Course(s) that formally assess(es) this program-level learning outcome: CSCI3157, CSCI3666 & CSCI3869					
Assessment Indicator(s) (taken from rubric)	**Teaching and learning activities**: List the most significant teaching and learning activities used by program faculty to facilitate the learning of this indicator in their class(es).	**Graded assignment(s) that formally assesses each indicator at its highest level**	**Performance expectations**: identify the percentage range for each level of performance by replacing the "xx's" below	**Average score for the indicator as a percent**	**How well did the students perform?**
Understanding attack and penetration strategy by identifying open ports using the netstat command. Using tools and utilities related to first stage – Reconnaissance And the second stage – Remuneration	Penetration testing process is introduced to the students. Students are taught how attackers plan their strategies to infiltrate into the systems of their target victims.	Individual (Hands-on-Lab)	Below expected levels: 0 – 69% At expected levels: 70– 89 % Above expected levels: 90– 100 %	66%	Choose one: ***Below expected levels** At expected levels Above expected levels
Network Design using Packet Tracer Tool	Students are introduced to the tool and the planning steps in using the OSI and TCP/IP Model. They were exposed to networking devices including switches and routers	Individual (Hands-on-Lab)	Below expected levels: 0 – 69% At expected levels: 70– 89 % Above expected levels: 90– 100 %	68%	Choose one: ***Below expected levels** At expected levels Above expected levels
Learn the different aspects of networking and how the Open Systems Interconnection (OSI) model works for communication between networks. Learn how to implement strategies to harden a system against network threats.	Client-server communication is introduced and students will learn how to setup the client service and server service using virtualization. They will need to write python scripts to simulate the communication between the client and the server	Group Project (Hands-on-Lab)	Below expected levels: 0 – 69% At expected levels: 70– 89 % Above expected levels: 90– 100 %	76%	Choose one: Below expected levels ***At expected levels** Above expected levels

1d. Overall Assessment Information of each Program-Level Learning Outcome

(Need to be submitted for each Assessment Indicator(s) in each Program-Level Learning Outcome)



PLO7 (Example)

Program-Level Learning Outcome: Evaluate and administer fundamental computer architecture, parallel organization, Internet based protocols and computer security technologies	
Course(s) that formally assess(es) this program-level learning outcome: CSCI3157	
Assessment Indicator: Understanding attack and penetration strategy by identifying open ports using the netstat command. Using tools and utilities related to first stage – Reconnaissance And the second stage – Remuneration	
Overall, how well did the students perform on this Program-Level learning outcome?	***Below expected levels** At expected levels Above expected levels
Analyze assessment of indicator results documented by the "Average score for the indicator as a percent" and "How well did the students perform?": What does the information in the previous reporting suggest to you about the performance expectations, the teaching strategies, and student learning?	Students performed below the expected level in CSCI 3157 due to the fact that too much materials is being covered in this course. Even though students are showing great interest to the subject especially when it comes to using tools for learning attack strategies.
Next steps: Plans for reinforcing effective teaching and learning strategies and for improving student learning (clearly identify what will be done, by whom, by when, and how you will assess the impact of the changes)	Continue implementing the teaching and learning strategies in place and look into the type and frequency of assessment of the PLO. Recommendations for changes will include revisiting the knowledge units mapping to course objectives. Creating a balanced cybersecurity courses will be required.
Projected quarter/semester of implementing "next steps"	Spring 2021
Results of "next steps" implementation–this section is to be completed the following year (describe how the implementation of the above "next steps" impacted teaching and learning in the program)	N/A
Suggestions for improving this report or process (if any)	N/A

1e. KU alignment

- Since our designation in 2015, our focus area was around Secure Software Development and hence, the Knowledge Units (KUs) Mappings were chosen to impart the necessary skills and abilities for the development of secure software (i.e., software that performs only its intended functions without the presence of exploitable vulnerabilities).
- In preparation for the re-designation process of 2021, the computer Science department at Florham is now using the new Knowledge Units (KUs) that can support future specialization areas in the field of Network Security Administration in addition to our current focus area of Secure Software Development.

1e. KU Alignment - Knowledge Units that are incorporated in our courses

Foundational
F1 - Cybersecurity Foundations (CSF)
F2 - Cybersecurity Principles (CSP)
F3 - IT Systems Components (ISC)

Technical Core
TC1 - Basic Cryptography (BCY)
TC2 - Basic Networking (BNW)
TC3 - Basic Scripting and Programming (BSP)
TC4 - Network Defense (NDF)
TC5 - Operating Systems Concepts (OSC)

Optional KUs – Selected in our PoS
O1 - Cyber Threats (CTH) - Non- Technical Core KU
O2 - Policy, Legal, Ethics, and Compliance (PLE) - Non-Technical Core KU
O3 - Advanced Network Technology and Protocols (ANT)
O4 - Software Assurance (SA)
O5 - Intrusion Detection / Prevention System (IDS)
O6 - Life-Cycle Security (LCS)
O7 - Software Security Analysis (SSA)
O8 - Network Security Administration (NSA)
O9 - Network Technology and Protocols (NTP)
O10 – Penetration Testing (PTT)
O11 – Vulnerability Analysis (VLA)
O12 - Algorithms (ALG)
O13 - Data Structures (DST)
O14 - Secure Programming Practices (SPP)

1e. Knowledge Unit (KU) Alignment CAE-CDE Course Mapping (2015 – 2020)

F: Cyber Security Foundational KUs (3 KUs)

TC: Technical Core KUs (5 KUs)

O: Optional KUs (Minimum of 14 optional KUs are required to meet the certification requirements)

	Knowledge Units	**CSCI1205**	**CSCI2215**	**CSCI2233**	**CSCI3315**	**CSCI3278**	**CSCI3304**	**CSC3157**	**CSCI3355**	**CSCI3666**	**CSCI3869**
F1	Cybersecurity Foundations (CSF)							X			
F2	Cybersecurity Principles (CSP)							X			
F3	IT Systems Components (ISC)						X	X		X	
TC1	Basic Cryptography (BCY)							X	X		
TC2	Basic Networking (BNW)									X	X
TC3	Basic Scripting and Programming (BSP)	X	X		X		X				
TC4	Network Defense (NDF)							X			X
TC5	Operating Systems Concepts (OSC)					X					
O1	Cyber Threats (CTH) - Non- Technical Core KU							X			
O2	Policy, Legal, Ethics, and Compliance (PLE) - Non-Technical Core KU							X			
O3	Advanced Network Technology and Protocols (ANT)									X	X
O4	Software Assurance (SAS)				X						
O5	Intrusion Detection / Prevention System (IDS)										X
O6	Life-Cycle Security (LCS)				X						
O7	Software Security Analysis (SSA)				X						
O8	Network Security Administration (NSA)									X	X
O9	Network Technology and Protocols (NTP)									X	X
O10	Penetration Testing (PTT)							X			X
O11	Vulnerability Analysis (VLA)							X			
O12	Algorithms (ALG)			X							
O13	Data Structures (DST)			X							
O14	Secure Programming Practices (SPP)	X	X		X						
		2	**2**	**2**	**5**	**1**	**2**	**9**	**1**	**5**	**7**

1e. Knowledge Unit (KU) Alignment CAE-CDE Course Mapping (starting Fall 2020)

Revised Mapping (Fall 2020) – Changes as part of Section IV – Continuous Improvement

Cybersecurity Program Changes for Fall 2020:

- Removed CSCI3315, CSCI3304
- Added two additional core cybersecurity course CSCI3158 & CSCI3870 in exchange of two computer science elective courses

	Knowledge Units	**CSCI1205**	**CSCI2215**	**CSCI2233**	**CSCI3278**	**CSC3157**	**CSCI3158**	**CSCI3355**	**CSCI3666**	**CSCI3869**	**CSCI3870**
F1	Cybersecurity Foundations (CSF)					X	X				X
F2	Cybersecurity Principles (CSP)						X				
F3	IT Systems Components (ISC)					X	X		X		X
TC1	Basic Cryptography (BCY)					X		X			
TC2	Basic Networking (BNW)								X	X	
TC3	Basic Scripting and Programming (BSP)	X	X								
TC4	Network Defense (NDF)					X				X	
TC5	Operating Systems Concepts (OSC)				X						
O1	Cyber Threats (CTH) - Non- Technical Core KU					X					X
O2	Policy, Legal, Ethics, and Compliance (PLE) - Non-Technical Core KU										X
O3	Advanced Network Technology and Protocols (ANT)								X	X	
O4	Digital Forensics (DFS)										X
O5	Intrusion Detection / Prevention System (IDS)									X	X
O6	Life-Cycle Security (LCS)						X				
O7	Network Forensics (NWF)										X
O8	Network Security Administration (NSA)						X		X	X	
O9	Network Technology and Protocols (NTP)								X	X	
O10	Penetration Testing (PTT)									X	
O11	Vulnerability Analysis (VLA)						X				
O12	Algorithms (ALG)			X							
O13	Data Structures (DST)			X							
O14	Secure Programming Practices (SPP)	X	X								
		2	**2**	**2**	**1**	**5**	**6**	**1**	**5**	**7**	**7**

1e. Knowledge Unit (KU) Alignment Course Outcomes Sample – CSCI3869

1) Student will cover potential threats to networks.

2) Students will learn how to implement strategies to harden system against network threats

3) Student will address the liability of the Network administrator for some crimes via the network.

4) Students will learn mitigation strategies for pursuit when system is compromised or data is altered, removed or copied.

5) Analyze problems, recommend solutions, products, and technologies to meet business objectives.

6) Recommend best security practices to achieve stated business objectives based on risk assumptions.

7) Actively protect information technology assets and infrastructure from external and internal threats.

8) Describe and discuss the security issues and implications of advanced and novel networks and protocols.

9) Identify and describe a variety of common network vulnerabilities.

10) Identify and mitigate security concerns at layer 2 and layer 3 of a network.

11) Students should be able to plan, organize and perform penetration testing on a simple network.

2. Students

- 2a. Student enrollment graduation in the PoS(s)
- 2b. Sample student certificate notation on transcript official letter
- 2c. Students Work Products (papers, assignments, labs, etc.)
- 2d Students Participation in Extracurricular Activities

3. Faculty Members

- 3a. Cyber Program(s) of Study POC + alternate POC
- 3b. Full-time, part-time, and adjunct faculty members + Faculty qualifications
- 3c. Faculty support of enrolled students
- 3d. Process of Faculty Promotion Reappointment (e.g. Faculty Policy Manual)

4. Continuous Improvement

- 4a. Continuous Improvement plan
- 4b. Continuous Improvement process
- 4c. Regular evaluation schedule

4a. Continuous Improvement plan

- Periodically preparing and implementing several action plans to enhance our program.
- Throughout the designation cycle from 2015 to 2020, we have encountered and resolved several shortfalls in our program.
- Implemented several Curricular changes for AYs 2015-2020

4a. Continuous Improvement plan

- In order to meet the new Knowledge Units (KUs) course mapping and to improve the quality of our courses, two new courses were developed for the cybersecurity concentration that will be required of all cybersecurity students starting fall 2020.
- The decision was primarily based on the following factors:
  - Learning outcome assessment results in CSCI 3157 & CSCI3666
  - CAE-CDE changes to the knowledge units as explained earlier
  - Streamlining course objectives, outcomes and topics and properly distribute the load and complexity of our existing courses
  - Ensuring learning outcomes mapping of knowledge units to our cybersecurity concentration courses

1e. Knowledge Unit (KU) Alignment CAE-CDE Course Mapping (starting Fall 2020)

Revised Mapping (Fall 2020) – Changes as part of Section IV – Continuous Improvement

Cybersecurity Program Changes for Fall 2020:

- Removed CSCI3315, CSCI3304
- Added two additional core cybersecurity course CSCI3158 & CSCI3870 in exchange of two computer science elective courses

	Knowledge Units	**CSCI1205**	**CSCI2215**	**CSCI2233**	**CSCI3278**	**CSC3157**	**CSCI3158**	**CSCI3355**	**CSCI3666**	**CSCI3869**	**CSCI3870**
F1	Cybersecurity Foundations (CSF)					X	X				X
F2	Cybersecurity Principles (CSP)						X				
F3	IT Systems Components (ISC)					X	X		X		X
TC1	Basic Cryptography (BCY)					X		X			
TC2	Basic Networking (BNW)								X	X	
TC3	Basic Scripting and Programming (BSP)	X	X								
TC4	Network Defense (NDF)					X				X	
TC5	Operating Systems Concepts (OSC)				X						
O1	Cyber Threats (CTH) - Non- Technical Core KU					X					X
O2	Policy, Legal, Ethics, and Compliance (PLE) - Non-Technical Core KU										X
O3	Advanced Network Technology and Protocols (ANT)								X	X	
O4	Digital Forensics (DFS)										X
O5	Intrusion Detection / Prevention System (IDS)									X	X
O6	Life-Cycle Security (LCS)						X				
O7	Network Forensics (NWF)										X
O8	Network Security Administration (NSA)						X		X	X	
O9	Network Technology and Protocols (NTP)								X	X	
O10	Penetration Testing (PTT)									X	
O11	Vulnerability Analysis (VLA)						X				
O12	Algorithms (ALG)			X							
O13	Data Structures (DST)			X							
O14	Secure Programming Practices (SPP)	X	X								
		2	**2**	**2**	**1**	**5**	**6**	**1**	**5**	**7**	**7**

Personal. Global. Transformational.

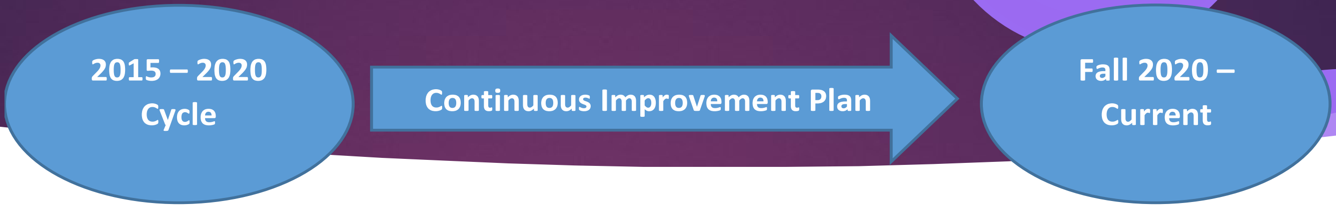
Becton College of Arts and Sciences Department of Math & Computer Science

Bachelor of Science in Computer Science Cybersecurity Concentration

Required Major Courses (30 Credits)	Required Cybersecurity Concentration Cources (18 Credits)
CSCI 1205 Introduction to Computer Programming (3) – C#	CSCI 3157 Cybersecurity (3)
CSCI 2215 Introduction to Computer Science (3) – C++	CSCI 3666 Data Communication and Computer Networks (3)
CSCI 2216 Introduction to Computer Science II (3)	CSCI 3158 Information Security Design and Mgm't (3)
CSCI 2255 Discrete Structures (3)	CSCI 3355 Intro to Cryptography (3)
CSCI 2233 Data Structures & Algorithms (3)	CSCI 3869 Network Security (3)
CSCI 3371 Computer Modeling & Simulation (3) or MATH 3300 Statistics (3)	CSCI 3870 Security Regulations, Detection & Forensics (3)
CSCI 3278 Operating Systems (3)	
CSCI 3315 Software Design (3)	
CSCI 3304 Computer Organizations (3)	
CSCI 4498 Internship (3)	

Courses in green cells are the newly aligned courses with KU

4a. Continuous Improvement plan



2015 – 2020 Cycle

Continuous Improvement Plan

Fall 2020 – Current

- Our Program of Study (PoS) enhancement will continue to involve the following criteria:

1. Selecting appropriate knowledge units to meet cybersecurity trends and the market demand including covering more specialization areas like network administration and software assurance.
2. Enhancing students' knowledge and experience in the cybersecurity concentration by improving the quality of courses by adopting properly aligned KUs and balanced course objectives, outcomes and topics.
3. Monitoring assessment results and performance indicators and adopt changes for continuous improvement to our program.

4b. Continuous Improvement process

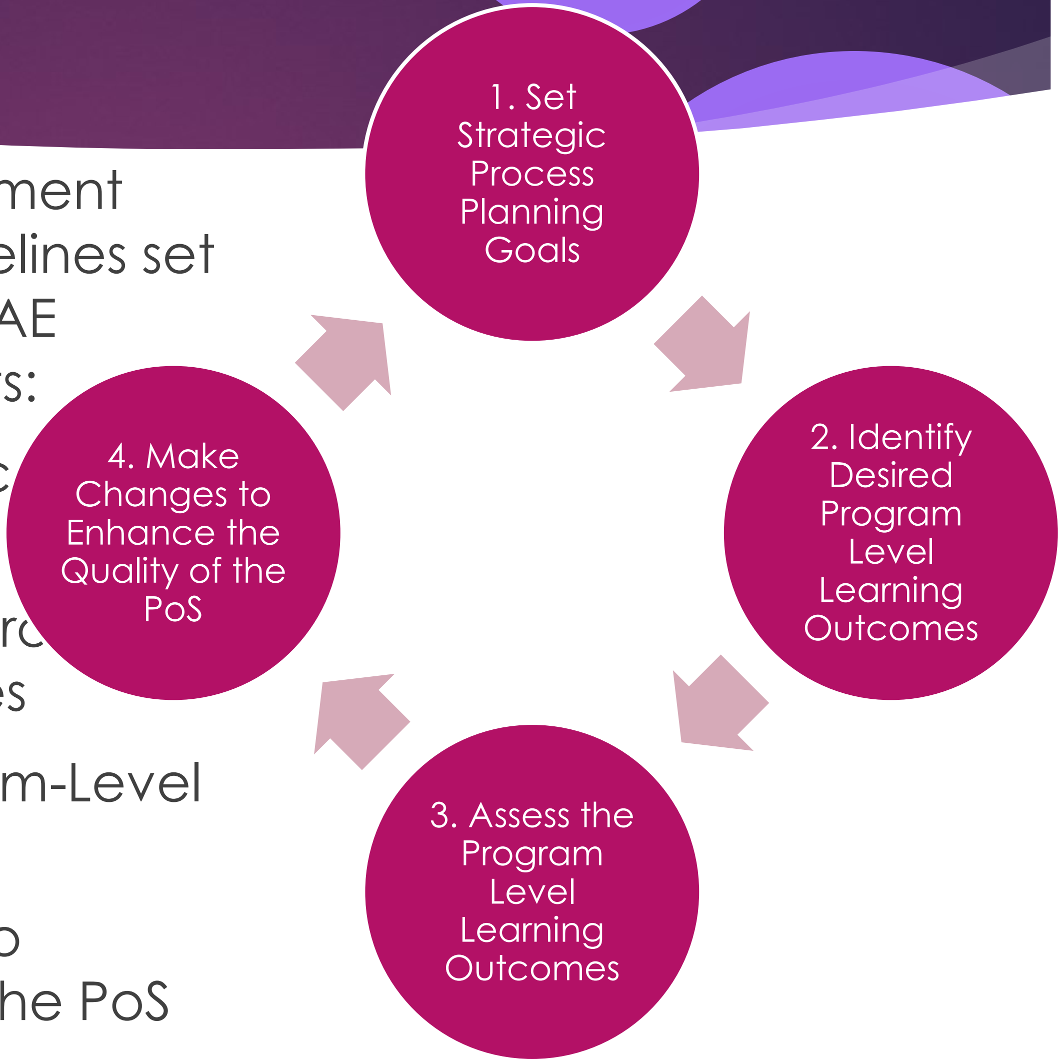
Our continuous improvement process follows the guidelines set by the proposed 2020 CAE designation requirements:

Step 1: Set strategic proc planning goals

Step 2: Identify Desired Prc Level Learning Outcomes

Step 3: Assess the Program-Level Learning Outcomes

Step 4: Make Changes to Enhance the Quality of the PoS



1. Set Strategic Process Planning Goals

2. Identify Desired Program Level Learning Outcomes

3. Assess the Program Level Learning Outcomes

4. Make Changes to Enhance the Quality of the PoS

4b. Continuous Improvement Process Step 1: Set strategic process planning goals

This is the initial step where several process-planning goals are being identified to ensure continuous monitoring and improvement of our PoS program. Goals are related to assessment improvement and PoS program adjustments. We have identified three important strategic process-planning goals listed as follows:

1. Enhance the quality of our concentration by adopting and modifying cybersecurity concentration courses.

2. Mapping to the newly released knowledge units.

3. Provide improved mapping to our program using desired program level learning outcomes.

4c. Regular evaluation schedule

To ensure continuous improvement of our program of study, we have utilized a regular evaluation schedule to address the following outcomes:

1. Meetings to evaluate our Program-level Learning Outcomes (PLO)
2. Enhancing our assessment indicators and other related metrics
3. Continuous improvement plan and process discussion and recommendations for appropriate changes and adjustments.

*** Full program evaluation occurs every two years and our regular evaluation meetings take place every semester, two meetings in the spring and two meetings in the fall**

Recommendations for Success

- Understand your PoS Curriculum
- Prepare your PoS Program-Level Learning Outcomes Carefully
- Design your courses to meet the PoS Learning Objectives
- Select the appropriate Knowledge Units that are aligned and mapped correctly to PoS related courses
- Plan your Assessment Indicators
- Perform Continuous Improvement to your PoS