Okaloosa Technical College

1976 Lewis Turner Blvd
Fort Walton Beach, FL 32547
Phone: (850) 833-3500
Fax: (850) 833-3466

Applied Cybersecurity Syllabus

Program Title: Applied Cybersecurity
Program Type: Career Preparatory
Career Cluster: Information Technology

Instructor: David Bricker
Email: david.bricker@okaloosaschools.com Phone: (850-217-1682)

Instructor: William "Bill" Williams
Email: william.williams@okaloosaschools.com Phone: (850-496-5407)

Program Description:

The purpose of this program is to prepare students for employment in the Cybersecurity field. The overall objectives and foundation for this course are built upon the Florida Department of Education (FDoE) Curriculum Framework for Applied Cybersecurity. The program structure below incorporates the FDoE requirements along with hands-on-skills. The FDoE requirements cover all objectives found in CompTIA Security+ certification. In addition to the FDoE requirements, this course integrates CENGAGE's Security+ Guide to Network Security Fundamentals book within the program as a Security+ study and preparation guide. At midway during the course, students are expected to obtain their CompTIA Security+ certification.

This program is knowledge and performance-based. Students will gain knowledge in cybersecurity fundamentals as well as hands-skills that translate directly to protecting business systems. The Security+ certification provides proof of knowledge, while the end-of-course certificate provides proof of hands-on skills.

CompTIA Security+ fulfills a baseline requirement for employment in many of the Department of Defense IT and Cybersecurity positions. CompTIA Security+ is a vendor-neutral certification with industry-wide recognition. Employers typically recognize that holders of a Security+ certification have a broad knowledge of security-related principles.

This program goes well beyond CompTIA Security+ and incorporates hands-on experience that includes industry standard cybersecurity hardening, monitoring of systems, and analysis of client configurations that will help the student meet employer's expectations.

Program Structure

This program is a planned sequence of instruction designed to meet two occupational completion points (OCPs) outlined in the FDoE. The students must complete OCP A plus one of the subsequent courses in OCP B that will be identified later in the course.

This program is comprised of courses which have been assigned course numbers in the SCNS (Statewide Course Numbering System) in accordance with Section 1007.24 (1), F.S. Career and Technical credit shall be awarded to the student on a transcript in accordance with Section 1001.44 (3)(b), F.S.

The following table illustrates the post-secondary program structure:

OCP	Course Number	Course Title	Course Length	SOC Code
A	CTS0018	Cybersecurity Associate	600 hours	15-1122
B	CTS0019	Information Security Manager	150 hours	15-1122
	or	or		
	CTS0021	Data Security Specialist	150 hours	
	or	**or**		
	CTS0060	Software Security Specialist	150 hours	
	or	**or**		
	CTS0085	Web Security Specialist	150 hours	
	or	**or**		
	CTS0089	Information Security Administrator	150 hours	

Common Career Technical Core – Career Ready Practices

Career Ready Practices describe the career-ready skills that educators should seek to develop in their students. These practices are not exclusive to a Career Pathway, program of study, discipline, or level of education. Career Ready Practices should be taught and reinforced in all career exploration and preparation programs with increasingly higher levels of complexity and expectation as a student advances through a program of study. The following lists are taken directly from the FDoE requirements:

1. Act as a responsible and contributing citizen and employee.
2. Apply appropriate academic and technical skills.
3. Attend to personal health and financial well-being.
4. Communicate clearly, effectively, and with reason.
5. Consider the environmental, social and economic impacts of decisions.
6. Demonstrate creativity and innovation.
7. Employ valid and reliable research strategies.
8. Utilize critical thinking to make sense of problems and persevere in solving them.
9. Model integrity, ethical leadership, and effective management.
10. Plan education and career path aligned to personal goals.
11. Use technology to enhance productivity.
12. Work productively in teams while using cultural/global competence.

Standards

After completing this program, the student will be able to perform the following:

01.0 Demonstrate knowledge, skill, and application of computer systems.
02.0 Demonstrate knowledge of different operating systems.
03.0 Develop a familiarity with the information technology industry.
04.0 Develop an awareness of microprocessors and digital computers.
05.0 Develop an awareness of programming languages.
06.0 Develop an awareness of emerging technologies.
07.0 Demonstrate an understanding of the Open Systems Interface (OSI) model.
08.0 Identify computer components and their functions.
09.0 Demonstrate proficiency using the Internet to locate information.
10.0 Demonstrate an understanding of Internet safety and ethics.
11.0 Demonstrate proficiency using common software applications.
12.0 Perform email activities.
13.0 Demonstrate proficiency in using presentation software and equipment.
14.0 Perform decision-making activities in a multimedia environment.
17.0 Demonstrate an understanding of cybersecurity, including its origins, trends, culture, and legal implications.
18.0 Describe the national agencies and supporting initiatives involved in cybersecurity.
19.0 Discuss the underlying concepts of terms used in cybersecurity.

20.0 Demonstrate an understanding of basic computer components, their functions, and their operation.
21.0 Demonstrate knowledge of different operating systems.
22.0 Demonstrate an understanding of the Open Systems Interface (OSI) model.
23.0 Describe the services and protocols that operate in the application, transport, network, and link layers of the OSI Model.
24.0 Demonstrate proficiency using computer networks.
25.0 Demonstrate an understanding of basic security concepts.
26.0 Demonstrate an understanding of legal and ethical issues in cybersecurity.
27.0 Demonstrate an understanding of virtualization technology.
28.0 Recognize and understand the administration of the following types of remote access technologies.
29.0 Understand the application of the following concepts of physical security.
30.0 Understand security concerns and concepts of the following types of devices.
31.0 Recognize and be able to differentiate and explain the following access control models.
32.0 Understand the security concerns for the following types of media.
33.0 Explain the following security topologies as they relate to cybersecurity.
34.0 Demonstrate an understanding of the technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges.
35.0 Demonstrate an understanding of common information and computer system security vulnerabilities.
36.0 Demonstrate an understanding of common cyber attack mechanisms, their consequences, and motivation for their use.
37.0 Be able to identify and explain the following different kinds of cryptographic algorithms.
38.0 Demonstrate an understanding of the following kinds of steganographic techniques and their use in cybersecurity.
39.0 Understand how cryptography and digital signatures address the following security concepts.
40.0 Understand and be able to explain the following concepts of PKI (Public Key Infrastructure).
41.0 Demonstrate an understanding of certificates and their role in cybersecurity.
42.0 Demonstrate an understanding of intrusion, the types of intruders, their techniques, and their motivation.
43.0 Demonstrate an understanding of Intrusion Detection Systems (IDS).
44.0 Describe host-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
45.0 Describe network-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
46.0 Demonstrate an understanding of IDS applications.
47.0 Demonstrate an understanding of port scanning and network traffic monitoring employed as intrusion detection techniques.
48.0 Demonstrate an understanding of firewalls and other means of intrusion prevention.
49.0 Demonstrate an understanding of vulnerabilities unique to virtual computing environments.
50.0 Demonstrate an understanding of social engineering and its implications to cybersecurity.
51.0 Demonstrate an understanding of fundamental security design principles and their role in limiting points of vulnerability.
52.0 Demonstrate an understanding of how to configure host systems to guard against cyber intrusion.
53.0 Demonstrate an understanding of authentication methods and strategies.
54.0 Demonstrate an understanding of methods and strategies for controlling access to computer networks.
55.0 Demonstrate an understanding of key network services, their operation, vulnerabilities, and ways in which they may be secured.
56.0 Demonstrate an understanding of the processes involved in hardening a computer system or network.
57.0 Demonstrate an understanding of Public Key Infrastructure (PKI) management functions, key states, and life cycle/transition considerations.
58.0 Demonstrate an understanding of the processes associated with assessing vulnerabilities and risks within an organization.
59.0 Demonstrate an understanding of penetration testing, the types of tests and metrics, testing methodologies, and reporting processes.
60.0 Demonstrate an understanding of the Incident Response Life Cycle and the activities comprising each phase.
61.0 Demonstrate proficiency in cybersecurity risk mitigation planning.
62.0 Demonstrate proficiency in establishing a risk management framework.
63.0 Demonstrate proficiency in creating a corporate security policy.
64.0 Demonstrate proficiency in addressing process risks.
65.0 Demonstrate proficiency in addressing physical security risks.
66.0 Demonstrate proficiency in cybersecurity contingency planning.
67.0 Demonstrate proficiency in cybersecurity disaster recovery planning.
68.0 Demonstrate proficiency in cybersecurity business continuity planning.
69.0 Demonstrate proficiency in the essential elements of forensic analysis.

70.0 Demonstrate an understanding of database design, structure, and operation.
71.0 Demonstrate a fundamental understanding of Structured Query Language (SQL).
72.0 Demonstrate an understanding of database security policies.
73.0 Demonstrate an understanding of database access control, functions, methods, and verification.
74.0 Demonstrate an understanding of database vulnerabilities, attack vectors, and associated countermeasures.
75.0 Demonstrate an understanding of pre- and post-intrusion actions to facilitate database recovery.
76.0 Demonstrate an understanding of software design, structure, and operation.
77.0 Demonstrate a fundamental understanding of common software attack vectors.
78.0 Demonstrate an understanding input syntax validation.
79.0 Demonstrate an understanding of best practices for processing input data to ensure safe and secure program code.
80.0 Demonstrate an understanding of the role of environment variables in the operation of software applications.
81.0 Demonstrate an understanding of program design strategies for inhibiting elevated privilege attacks.
82.0 Demonstrate an understanding of the primary security services used in Internet and intranet environments.
83.0 Demonstrate a fundamental understanding of the SSL protocol stack and its elements.
84.0 Demonstrate an understanding of IPSec, including its uses, elements, and mechanisms.
85.0 Demonstrate an understanding of S/MIME, including its uses, functions, cryptographic algorithms, and key certificates.
86.0 Demonstrate an understanding of Kerberos and its role in third-part authentication in a distributed network.
87.0 Demonstrate an understanding of identity management and ways in which secure identify information is exchanged across different domains.
88.0 Complete a safety skills inventory.
89.0 Demonstrate acceptable project values.
90.0 Demonstrate the ability to detect and resolve system vulnerabilities.
91.0 Plan, organize, and carry out a penetration testing plan.
92.0 Demonstrate proficiency in conducting forensic analysis.
93.0 Successfully work as a member of a team.
94.0 Manage time according to a plan.
95.0 Keep acceptable records of progress problems and solutions.
96.0 Manage resources.
97.0 Use tools, materials, and processes in an appropriate and safe manner.
98.0 Research content related to the project and document the results.
99.0 Use presentation skills, and appropriate media to describe the progress, results and outcomes of the experience.
100.0 Demonstrate competency in the area of expertise related to the Applied Cybersecurity education program previously completed that this project is based upon.

Hands-on Labs:

The following labs will be used to support the FDoE Curriculum and the CompTIA foundations:

1. TestOut (Online Training Lab)
   - See TestOut Syllabus for full content listing
2. Hands-on with the SecurityOnion:
   - Linux basics
   - Intrusion Detection basics
   - Security Event Information Management system (SEIM) basics
3. Marcraft Lab
   - Infrastructure Security and Surveillance Systems
   - Local Computer Security Options
   - Network Security Essentials
   - Implementing Cyber Security
   - Enterprise Network Security Systems
   - Industrial and Utility Network Security
   - Medical Network Security
   - Introduction to Ethical Hacking
4. Malware Lab

- Introduction to malware (live malware analysis)

5. System Hardening Lab
   - Securely configuring systems (harden) per NIST and\or CIS guidelines.

Note: Students will progress through each of the above labs at their own pace. Each of the above labs must be completed to receive a passing score and an end-of-course certificate.

Equipment/Supplies:

Students will provide:

- Notebooks and writing utensils if desired (Electronic capture of notes encouraged).

OTC or Instructor Will Provide:

- Lab Equipment and Software
- Computer Systems
- Specific note taking computer applications
- Selections from other documents and manuals
- Other handouts as required
- User Agreement and rules for Lab

Note: all documents, assignments, and quizzes are electronic.

Daily Class Organization and Structure

Each day begins and ends with standard events designed to prepare the student for cyber activities in the workplace. In-between these standard events, the course work will vary widely, and each student may be on separate learning tracks. Learning tracks include hands-on lab work, research, or classroom lecture. Typical daily events include:

5:00 PM – Class start. Students prepare classroom study area/ and review assigned cyber feeds and podcasts
- Daily Cyber Podcast (normally https://www.thecyberwire.com/)
- Assigned RSS Cyber Security Feeds (RSS links include U.S. Cert, NIST, Krebs, and Schneier)

5:15 PM – As a group, student's discuss the day's cyber feeds/podcasts.
5:30 PM – Perform assigned lab work or attend a lecture (as scheduled).
6:30 PM – 15 Min Break
6:45 PM – Perform lab work
7:30 PM – 30 Minute Lunch
8:00 PM – Perform lab work
8:30 PM – Per schedule & track (Assigned lab work or Sec+ exam group Study)
9:40 PM – Students perform cybersecurity tasks to secure classroom and study area
9:45 PM – Class ends

Overall Course Grading Criteria and Requirements:

Grades results are a combination of participation, research assignments, quizzes, tests, and labs.
5% - Class participation
10% - Research Assignments
15% - Tests & Quizzes
70% - Lab Performance & Completion (hands-on performance matters most)

_____
100%

Communication

This course will use a Learning Management System (LMS) as a document repository and document generation tool.

Access to course assignments, internal quizzes, documents, and grade book is via the designated LMS. On the first day of class, students will navigate to a link sent by the instructors for the student to visit and request access.

The LMS will also serve as the place for online discussions. The majority of interaction is in the classroom, but for those instances where online communication is applicable, we'll use the LMS as a collaborative tool.

Online quizzes

There are two sources for online quizzes: TestOut (http://wwwnew.testout.com) which is included with this course and is a primary source for student practice exams. The LMS also serves as the secondary exam source which contains instructor developed quizzes. More details will follow in an expanded syllabus.

CompTIA Security+ Examination SY0-501

This course includes preparation for the CompTIA Security+ SY0-501 certification. When the student is ready and approved by the instructor, the student will use a voucher provided by the school to take their exams. There is only one voucher provided for each student. Should a student fail the exam, a second voucher is available to the student at a reduced cost. Coordination of the secondary voucher is through the voucher vendor.

Type of Questions: Multiple choice and performance-based
Allowed Test Time: 90 Minutes
Passing Score: 750 (on a scale of 100-900).

Students can take their Security+ examinations beginning in Jan 2020, and all students are expected to have their Security+ examinations completed no later than 1 Mar 2020. Student's that plan to take the exam before January 2020 should confer with an instructor to obtain approval and their voucher. Students will keep instructors aware of Security+ examination test registration, schedules, and completion. Upon completion of the Security+ exam, the student shall use the CompTIA public share link to publish exam results for instructors to review.

Course Grading Scale

90% and above	=	A
80% - 89.9%	=	B
70% - 79.9%	=	C
60% - 69.9%	=	D (no certificate; D or below is not capable of protecting systems or networks)
59.9% and below	=	F

Research Assignments and Other Tasks

1. Students will complete research assignments on current cybersecurity trends or events.
2. Review of cybersecurity podcasts and RSS feeds are essential components to global threat situational awareness.
3. Students will complete individual and team assignments.
4. Students must satisfactorily perform hands-on system hardening (applying secure system configurations).
5. Students will provide cyber-related presentations to the class on assigned topics.
6. Students will complete an introduction to resumes, applications, and job interviews.

Skill Assessment Rubric

Each hands-on skill assignment is aligned to meet specific FDoE standards or requirements. A specific grading rubric is provided for each hands-on task in the format shown here:

Criterion	Possible Points	Points Earned
The hands-on tasks are completed in minimum time and provide the minimum results or information per the standard.	Total task (+ subtask) = 100 points.	

Tasks may be broken down into subtasks each with criteria and specified points as part of the total points.	Subtask points.	

Make-up Policy

All testing and assessments will be scheduled per course syllabus. Makeup work is typically not allowed unless an instructor gives prior approval. The student should coordinate planned absences with the instructors. The instructor may assign additional outside work to be completed for each absence.

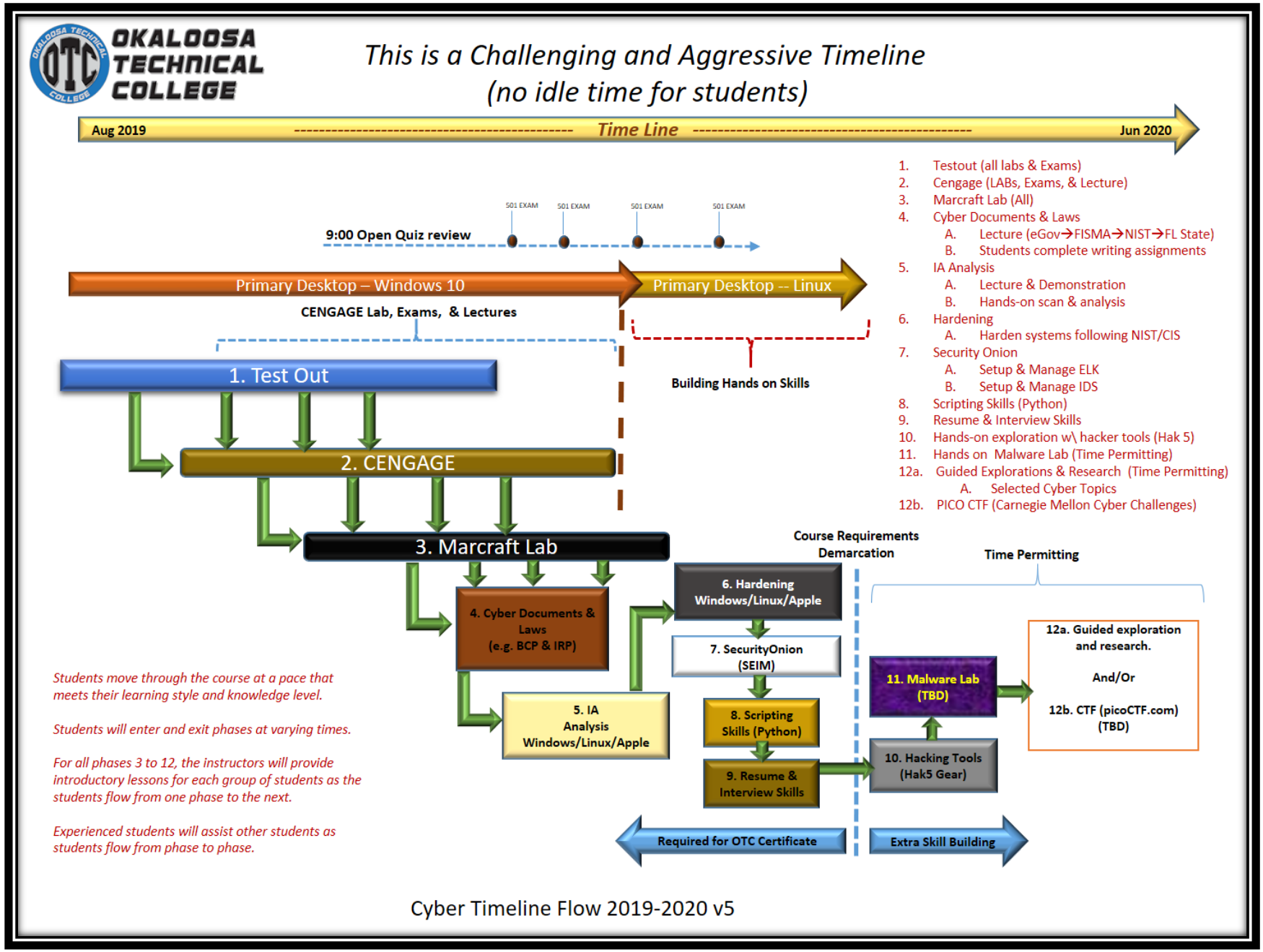
Attendance

See Student Handbook for attendance policies. Attendance is not only expected but vital to a student's success.

End of course Certificate

To receive the end-of-course certificate, the student must complete these milestones:

1. Complete all videos and exams in TestOut lab with all examinations corrected to 100%.
2. Complete instructor assigned quizzes and assignments.
3. Demonstrate proficiency in completing all stations of the Marcraft lab.
4. Demonstrate proficiency in establishing an instance of SecurityOnion with an operational Intrusion Detection System.
5. Demonstrate proficiency in establishing an instance of SecurityOnion with an operational (SEIM) that is processing client events and logs.
6. Complete Security+ examination (or at least the student made one attempt of the examination).
7. Demonstrate proficiency in system hardening.
8. Demonstrate basic proficiency with the Microsoft Windows and Linux Operating Systems.



Cyber Timeline Flow 2019-2020 v5