Department of Education | College, Career and Technical Education

Published for 2020-21 school year.

Cybersecurity Practicum

Primary Career Cluster:	Information Technology (IT)
Course Contact:	CTE.Standards@tn.gov
Course Code(s):	C10H21
Prerequisite(s):	*Algebra I* (G02X02, G02H00) and *Cybersecurity II*
Credit:	1
Grade Level:	11-12
Focus Elective Graduation Requirements:	This course satisfies one of three credits required for an elective focus when taken in conjunction with other *Information Technology* courses.
Program of Study (POS) Concentrator:	This course satisfies one out of two required courses that meet the Perkins V concentrator definition, when taken in sequence in the approved program of study.
Programs of Study and Sequence:	This is the capstone course in the *Cybersecurity* program of study.
Aligned Student Organization(s):	SkillsUSA: http://www.tnskillsusa.com Technology Student Association (TSA): http://www.tntsa.org
Available Student Industry Certifications:	Students are encouraged to demonstrate mastery of knowledge and skills learned in this course by earning the appropriate, aligned department-promoted industry certifications. Access the promoted list here for more information.
Teacher Endorsement(s):	037, 041, 055, 056, 057, 152, 153, 203, 204, 311, 413, 434, 435, 436, 470, 474, 475, 476, 477, 582, 595, 740, 742
Required Teacher Certifications/Training:	All endorsements except for 742 will require either the NOCTI test code 5906: Computer Programming certification or the equivalent of twelve semester hours of computer course work including at least six hours of programming language. If students are assigned in work-based learning settings, teachers must attend WBL training and earn the WBL Certificate provided by the Tennessee Department of Education.
Teacher Resources:	https://www.tn.gov/education/career-and-technical-education/career-clusters/cte-cluster-information-technology.html

Course Description

Cybersecurity Practicum is a capstone course intended to provide students with the opportunity to apply the skills and knowledge learned in previous *Cybersecurity* courses toward the completion of an in-depth project with fellow team members. Students who have progressed to this level in the program of study

take on more responsibilities for producing independent work and managing processes involved in the planning, designing, refinement, and production of cybersecurity applications. Upon completion of the practicum, proficient students will be prepared for postsecondary study and career advancement in cybersecurity, and will be equipped to market their finished product should they choose.

Work-Based Learning Framework

Practicum activities may take the form of work-based learning (WBL) opportunities (such as internships, cooperative education, service learning, and job shadowing) or industry-driven project-based learning. These experiences must comply with the Work-Based Learning Framework guidelines established in SBE High School Policy 2.103. As such, this course must be taught by a teacher with an active WBL Certificate issued by the Tennessee Department of Education and follow policies outlined in the Work-Based Learning Policy Guide available online at https://www.tn.gov/education/career-and-technical-education/work-based-learning.html. The Tennessee Department of Education provides a *Personalized Learning Plan* template to ensure compliance with the Work-Based Learning Framework, state and federal Child Labor Law, and Tennessee Department of Education policies, which must be used for students participating in WBL opportunities.

Program of Study Application

This is the fourth course in the *Cybersecurity* program of study. For more information on the benefits and requirements of implementing this program in full, please visit the Information Technology website at https://www.tn.gov/education/career-and-technical-education/career-clusters/cte-cluster-information-technology.html.

Course Requirements

This capstone course aligns with the requirements of the Work-Based Learning Framework (established in Tennessee State Board High School Policy), with the Tennessee Department of Education's Work-Based Learning Policy Guide, and with state and federal Child Labor Law. As such, the following components are course requirements:

Course Standards

1) A student will have a Personalized Learning Plan that identifies their long-term goals, demonstrates how the Work-Based Learning (WBL) experience aligns with their elective focus and/or high school plan of study, addresses how the student plans to meet and demonstrate the course standards, and addresses employability skill attainment in the following areas:
    a. Application of academic and technical knowledge and skills (embedded in course standards)
    b. Career knowledge and navigation skills
    c. 21st Century learning and innovation skills
    d. Personal and social skills

Cybersecurity Career Planning

2) Research a company or organization that utilizes cybersecurity applications or specializes in cybersecurity solutions. Companies could range from large software developers, to niche organizations that retain specialists on staff to serve their particular clients' needs. For the chosen company, cite specific textual evidence from the company's literature, as well as available press coverage (if available) to summarize:
    a. The mission and history of the organization
    b. Headquarters and organizational structure
    c. Products or services provided
    d. Credentials required for employment and how they are obtained and maintained
    e. Policies and procedures
    f. Reports, newsletters, and other documents published by the organization
    g. Website and contact information

3) Analyze the requirements and qualifications for various cybersecurity job postings identified from specific company websites or online metasearch engines. Gather information from multiple sources, such as sample resumes, interviews with professionals, and job boards, to determine effective strategies for realizing career goals. Create a personal resume modeled after elements based on the findings above, then complete an authentic job application as part of a career search or work-based learning experience.

4) Participate in a mock interview. Prior to the interview, research tips on dress and grooming, most commonly asked interview questions, appropriate conduct during an interview, and recommended follow-up procedures. Upon completion of the interview, write a thank you letter to the interviewer in a written or email format.

Professional Ethics and Legal Responsibilities

5) Investigate current issues surrounding cybersecurity and its applications. Explore a range of arguments concerning privacy rights as they relate to the mining of personal data; determine when it is ethical and legal to collect data for profit versus for security purposes. Advance an original argument that debates the pros and cons and summarizes the potential ramifications for clients, users, the public, and one's own personal reputation, drawing on evidence gathered from news media, company policies, and state and federal laws.

6) Research a case study involving an ethical issue related to intellectual property rights. Examine a variety of perspectives surrounding the issue, then develop an original analysis explaining the impact of the issue on those involved, using persuasive language and citing evidence from the research. Potential issues include copyright infringement, piracy, plagiarism, art licensing, creative commons, and the state/federal laws that govern them.

Course Project

In teams, students will complete the capstone security assessment to help identify gaps and provide mitigating solutions of a fictitious small and medium-sized business (SMB) that is concerned over their security posture of their business. This assessment should span the various types of tests and attack vectors that students learned about in previous courses in the program of study. The project must provide opportunities for members to experience a high level of interactivity related to the challenges of learning

and applying advanced skills in cybersecurity. The project must provide a safe, legal, and ethically sound environment with up-to-date facilities and equipment.

7) Research and investigate how policies and procedures are used to define the practices within the business and how are they are used to define the practices within the business as they relate to information security. Create three policies that will help establish a solution to potential security concerns:
    a. Create an administrative policy, based on this research that employees would need to follow to have access to system resources, or password usage.
    b. Create a technical policy that defines how a technical control helps to protect an organization. For example, define how the IT department must configure a firewall.
    c. Create a control policy for the physical controls for the organization. For example, a policy to define the physical access to the IT equipment to help contain unauthorized access to the firewall and or routers.

8) Analyze a technical security solution scenario and determine what solution could be deployed to help mitigate an issue and protect the organization against malware infections.

9) Test and run a vulnerability assessment on the SMB to determine what vulnerabilities exist on a resource (server, network device, computer, etc.) using Nessus. Students will run a scan on a computer find the vulnerabilities, and preform the mitigating steps to remove the identified vulnerabilities.

Communication of Project Results

10) Upon completion of the practicum, develop a technology-enhanced presentation showcasing their findings and solutions, highlights, challenges, and lessons learned from the experience to a small volunteer panel of professionals that could serve as the fictitious business owners. The presentation should be delivered orally, but supported by relevant graphic illustrations, such as diagrams, flowcharts, and/or market data on the target users. Prepare the presentation in a format that could be presented to both a technical and a non-technical audience, as well as for a career and technical student organization (CTSO) or CyberPatriot competitive events.

Portfolio

11) Create a portfolio, or similar collection of work, that illustrates mastery of skills and knowledge outlined in the previous courses and applied in the practicum. The portfolio should reflect thoughtful assessment and evaluation of the progression of work involving the application of steps of the design process, as outlined by the instructor. The following documents will reside in the student's portfolio:
    a. Personal code of ethics
    b. Career and professional development plan
    c. Resume
    d. Project proposal with supporting documents
    e. List of responsibilities undertaken through the course
    f. Examples of visual materials developed and used during the course (such as drawings, models, presentation slides, videos, and demonstrations)
    g. Marketing plan

h. Description of technology used, with examples if appropriate
i. Periodic journal entries reflecting on tasks and activities
j. Feedback from instructor and/or supervisor based on observations

Standards Alignment Notes

*References to other standards include:

- P21: Partnership for 21st Century Skills Framework for 21st Century Learning
    - Note: While not all standards are specifically aligned, teachers will find the framework helpful for setting expectations for student behavior in their classroom and practicing specific career readiness skills.