Department of Education | College, Career and Technical Education

May 2023

Cybersecurity II

Primary Career Cluster:	Information Technology (IT)
Course Contact:	CTE.Standards@tn.gov
Course Code(s):	C10H20
Prerequisite(s):	*Cybersecurity I*
Credit:	1
Grade Level:	11
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 third course in the *Cybersecurity* program of study.
Aligned Student Organization(s)	SkillsUSA: http://www.skillsusatn.org/ Technology Student Association (TSA): http://www.tntsa.org
Coordinating Work-Based Learning:	Teachers are encouraged to use embedded WBL activities such as informational interviewing, job shadowing, and career mentoring. For information, visit https://www.tn.gov/education/educators/career-and-technical-education/work-based-learning.html.
Promoted Student Industry Credentials	Credentials are aligned with post-secondary and employment opportunities and with the competencies and skills that students acquire through their selected program of study. For a listing of promoted student industry credentials, visit https://www.tn.gov/content/tn/education/educators/career-and-technical-education/student-industry-certification.html.
Teacher Endorsement(s):	037, 041, 055, 056, 057, 152, 153, 173, 203, 204, 311, 413, 434, 435, 436, 470, 474, 475, 476, 477, 582, 595, 740, 742, 952, 953
Required Teacher Certifications/Training:	All endorsements except for 173 and 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.
Teacher Resources:	https://www.tn.gov/education/educators/career-and-technical-education/career-clusters/cte-cluster-information-technology.html Best for All Central: https://bestforall.tnedu.gov/

Course at a Glance

CTE courses provide students with an opportunity to develop specific academic, technical, and 21st century skills necessary to be successful in career and in life. In pursuit of ensuring every student in Tennessee achieves this level of success, we begin with rigorous course standards which feed into intentionally designed programs of study.

Students engage in industry relevant content through general education integration and experiences such as career and technical student organizations (CTSO) and work-based learning (WBL). Through these experiences, students are immersed with industry standard content and technology, solve industry-based problems, meaningfully interact with industry professionals, and use/produce industry specific, informational texts.

Using a Career and Technical Student Organization (CTSO) in Your Classroom

CTSOs are a great resource to put classroom learning into real-life experiences for your students through classroom, regional, state, and national competitions, and leadership opportunities. Below are CTSO connections for this course, note this is not an exhaustive list.

- Participate in CTSO Fall Leadership Conference to engage with peers by demonstrating logical thought processes and developing industry specific skills that involve teamwork and project management.
- Participate in contests that highlight job skill demonstration, interviewing skills, community service activities, extemporaneous speaking, and job interview.
- Participate in leadership activities such as Student2Student Mentoring, National Week of Service, Officer Training, and Community Action Project.

For more ideas and information, visit Tennessee SkillsUSA at: http://www.skillsusatn.org/.

Using Work-Based Learning (WBL) in Your Classroom

Sustained and coordinated activities that relate to the course content are the key to successful work-based learning. Possible activities for this course include the following. This is not an exhaustive list.

- **Standards 1.1-3.2** | Invite a local attorney to explain the legal and ethical concepts and threats involved with cybersecurity.
- **Standards 4.1-4.3** | Have an industry rep discuss the importance of cryptology.
- **Standards 5.1-6.3** | Job shadow a cybersecurity policy director.
- **Standards 7.1-9.1** | Integrated project with interactions with industry professionals.

Course Description

Cybersecurity II challenges students to develop advanced skills in concepts and terminology of cybersecurity. This course builds on previous concepts introduced in Cybersecurity I while expanding the content to include malware threats, cryptography, wireless technologies, and organizational security. Upon completion of this course, proficient students will be able to demonstrate an understanding of cybersecurity ethical decisions, malware threats, how to detect vulnerabilities, principles of cryptology, security techniques, contingency plan techniques, security analysis, risk management techniques, and advanced methods of cybersecurity.

Course Standards

1. Legal and Ethical Concepts in Cybersecurity

1.1 Legislation: Drawing from various resources, analyze **current legislation that governs computer related crimes**. For example, create a presentation discussing common computer crimes, terms of use, and legal issues such as copyright laws, fair use laws, and trademark ethics pertaining to images, videos, and recorded sounds.

1.2 Acts of Computer Crime: Using news articles, research and report on **current legal cases involving acts of computer crime**. For example, research and report on a recent case of computer fraud, piracy, and abuse.

1.3 Evidence Collection: Consult a variety of sources to analyze **methods used to discover method of evidence collection to support legal cases involving computer related crime**. Create a presentation highlighting methods used.

2. Malware Threats

2.1 Forms of Malware: Conduct research to **determine various forms of malware**. Give specific examples and create an infographic highlighting the different types.

2.2 Methods to Handle Malware: Analyze **methods to handle malware**, such as how to control access to secured resources and computer resources. Give specific examples of methods that a security analyst can use, like encryption techniques, basic input/output system (BIOS) features, and strategies for dealing with malware.

3. Threats and Vulnerabilities

3.1 Types of Attacks: Analyze and differentiate among various **types of attacks on systems and networks**. Create a table or other graphic organizer that lists the following types of attacks and details their purposes and characteristics. Different types of attacks can include but are not limited to:

a. virus,
b. worms,
c. trojans,
d. unpatched software,
e. password cracking,

f. advanced persistent threat,
g. reconnaissance/footprinting,
h. infiltration,
i. network breach,
j. network exploitation,
k. attack for effects (e.g., deceive, disrupt, degrade, and destroy),
l. DoS/DDoS, session hijacking,
m. HTTP spoofing,
n. DNS attacks,
o. switch attacks,
p. man-in-the-middle (MITM) attacks,
q. cross site scripting, and
r. drive-by-attacks.

3.2 Attack Methods: Consult a variety of sources to **research attack methods** and create a **report on at least two events**. For example, show how social engineering (e.g., baiting, phishing/spear phishing, pretexting/blagging, tailgating, quid pro quo, etc.) led to the breach of an organization.

4. Principles of Cryptology

4.1 Cryptology Tools: Research and create an information artifact (e.g., brochure, fact sheet, or narrative) **analyzing cryptographic tools, procedures for use, and products** including but not limited to: PKI, Certificates, PGP, and Certificate authorities.

4.2 Public Key Infrastructures: In teams, examine trade journals and research literature from product vendors to **develop a simple public key infrastructure to be used by a small business**. For example, show how an organization can use digital certificates, encrypted file transfers, and email utilizing encryption.

4.3 Self-Signed Certificate: Investigate and demonstrate **the creation of a self-signed certificate for use on a web server by using command line or online tools**. For example, create, install, secure, backup, and restore a certificate.

5. Wireless Security Techniques

5.1 Wireless Attack Methods: Analyze **attack methods on wireless networks**. Read and interpret trade journals, assessing the usefulness of each source, to **describe the different methods used**. For example, cite evidence from trade journals to explain man in the middle, sniffing, and wireless SSID spoofing to explain their unique attack methods.

5.2 Wireless Security Protocols: Demonstrate **the use of wireless security protocols**. Drawing on evidence from textbooks and other resources, **evaluate the capabilities of WPA, WPA-2, and WEP, and the effectiveness of the security protocols** and demonstrate how to use them appropriately.

6. Organizational Security Techniques

6.1 Environmental Controls: Consult a variety of sources to analyze, define, and demonstrate **the use of environmental controls**. Instructional material may include textbooks, manuals, websites, video tutorials, and more. For example, show how BIOS sets controls on a system.

6.2 Security Operations: As a class, work collaboratively to develop simple **policies that support the operations of security in an organization**. For example, create an email security policy that outlines rules regarding responsible technology use.

6.3 Security Awareness: Research and analyze **security awareness in an organization**. Create a table or other graphic organizer that lists the following examples of **how to manage user habits and expectations**:

a. security policy training and procedures;
b. personally identifiable information;
c. information classifications;
d. data labeling, handling, and disposal;
e. compliance with laws, best practices, and standards;
f. user habits;
g. threat awareness; and
h. use of social networking.

7. Contingency Planning Techniques

7.1 Impact of Security Incidents: Synthesize information from a range of sources to analyze and **define the impact of security incidents on an organization**. For example, describe the various types of incidents including but not limited to malware, intrusion, and other forms of compromise.

7.2 Disaster Recovery Plan: Research and define **what is disaster recovery (DR) plan is and how to develop one**. For example, develop a step by step guide on how an organization would recover from an incident. The disaster recovery plan should highlight three key aspects: preventive measures, detective measures, and corrective measures. Write a justification that explains to a client why a disaster recovery plan is important.

8. Security Analysis Evaluation

8.1 Assessment Methods: Explore and identify various **assessment methods including but not limited to network penetration and vulnerability testing**. Create a chart to define how these systems are designed to help identify weak links in a company's cybersecurity chain, and how they provide feedback and recommendations needed in order to address them.

8.2 Security Testing Tools: Identify and explain **the uses for security testing tools**. Demonstrate and compare the effectiveness of Nessus and Nmap. Write and explanation and justify conclusions by citing supporting evidence from technical manual vendor resources.

8.3 Security Analysis: Demonstrate each of the following concepts:
   a. Evaluate the **patch status of a machine**.
   b. Demonstrate knowledge of **packet-level analysis** in order to install and view packets.
   c. Perform **secure data destruction** (e.g., Secure Erase, BCWipe).

9. Advanced Methods of Cybersecurity

9.1 Network Configuration: Utilizing prior fundamentals, demonstrate **proper secure network configuration and administration**. For example, use common tools and design a network utilizing secure protocols, and evaluate the network upon completion. The plan should address, but is not limited, to the following:
   a. Applying and implementing secure network administration principles.
   b. Demonstrating knowledge of how network services and protocols interact to provide network communications in order to securely implement and use common protocols.
   c. Identifying commonly used default network ports.
   d. Setting up a Network Address Translation (NAT) device.
   e. Configuring a Virtual Private Network (VPN).
   f. Configuring a remote access policy Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).
   g. Demonstrating knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol (TCP/IP)), Dynamic Host Configuration Protocol (DHCP) and directory services (e.g., Domain Name System (DNS) by setting up common protocols, e.g., Secure Shell (SSH), netstat, Simple Mail Transfer Protocol (SMTP), nslookup, Telnet, DNS/Bind, FTP, IIS/Web Pages, DHCP/DNS server).
   h. Locating open ports by completing a port scan.
   i. Demonstrating the knowledge and use of network statistics (netstat).

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.