Department of Education | College, Career and Technical Education

Pending Approval for 2021-22 school year.

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.tnskillsusa.com 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/content/tn/education/career-and-technical-education/work-based-learning.html
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, 952, 953
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
Teacher Resources:	https://www.tn.gov/education/career-and-technical-education/career-clusters/cte-cluster-information-technology.html

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 demonstrate and 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 .

Program of Study Application

This program offers a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and cybersecurity-related careers in the Information Technology career cluster. This is the third 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 Standards

Legal and Ethical Concepts in Cybersecurity

1) 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.

2) 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.

3) Consult a variety of sources to analyze techniques used to discover method of evidence collection to support legal cases involving computer related crime. Create a presentation highlighting methods used.

Threats and Vulnerabilities

4) 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
r. Drive-by-attacks

Principles of Cryptology

5) Research analyzing cryptographic tools, procedures for use, and products including but not limited to: PKI, Certificates, PGP, and Certificate authorities. Implement the ability to use at least one of the techniques discovered.

6) 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.

7) 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.

Wireless Security Techniques

8) 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.

9) 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.

Organizational Security Techniques

10) 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.

11) 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.

12) 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
    h. Use of social networking

Contingency Planning Techniques

13) 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.

14) 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.

Security Analysis Evaluation

15) 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 cyber security chain and how they provide feedback and recommendations needed in order to address them.

16) 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 manuals vendor resources.

17) 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).
    d. Description (and/or demonstration) of using Kali Linux to explore, analyze, and assess a test network

Advanced Methods of Cybersecurity

18) Utilizing prior fundamentals, demonstrate proper secure network configuration and administration regarding ports and routing tables:
    a. Identifying commonly used default network ports.
    b. Locating open ports by completing a port scan, and demonstrating competency in closing and opening ports on Windows and Linux computers.
    c. Setting up a Network Address Translation (NAT) device.
    d. Defining custom entries in a router table and/or creation of custom subnetting, either on a client or on a router.

19) Utilizing prior fundamentals, demonstrate proper secure network configuration and administration of the following communication capabilities/protocols:
    a. Configuring a Virtual Private Network (VPN).
    b. Configuring a remote access policy Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP) or similar protocol.
    c. Demonstrating knowledge of key network protocols such as Transmission Control Protocol and Internet Protocol (TCP/IP), Dynamic Host Configuration Protocol (DHCP), directory services (e.g., Domain Name System (DNS)), and Simple Mail Transfer Protocol (SMTP).

20) Utilizing prior fundamentals, demonstrate proper secure network configuration and administration, 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. Demonstrating the knowledge and use of network statistics (netstat), and network maps such as that generated by Zenmap and similar utilities.

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.