Computer Engineering V:
Cybersecurity and Hacker Defense

First Semester

Course Information

Grade(s):	12
Discipline/Course:	Technology Education
Course Title:	Computer Engineering V: Cybersecurity and Hacker Defense, Semester I
Prerequisite(s):	Computer Engineering IV: Networking and Troubleshooting (Full Year) *or* Computer Engineering IV: Networking and Troubleshooting (Semester) with teacher's permission
Course Description: *Program of Studies*	Students will learn how to construct, manage, use and defend a server in this culminating level course. This course will dive into computer and cyber security. Students will further develop, analyze, and apply skills related to Security + certification.Focus in this course will be on advanced networking, network security and hardware as well as encryption, security and managing a Windows server. Students will learn to protect a system from viruses and thwart hackers. The content of this course is aligned with CompTIA Security+ standards.
Course Essential Questions:	● What necessary precautions must people in today's digital connected world take in order to protect themselves from harm? ● How do risk, risk management, and risk assessment systems affect the social and business structures of our world? ● Why must we use security systems for any time we are transferring or storing data? ● Why is account and access management so important to network security? ● What vulnerabilities are there in networked systems? ● How does having a variety of system options and different vulnerabilities affect the cyber security industry?
Course Enduring Understandings:	● A digital footprint can last forever and negatively impact one's reputation. ● Cyberbullying is done by participants to anonymously take advantage of others. ● There are many things one can do to stay safe online ● Explain Information Literacy and affective search principles

	• It is important to give proper Creative Credit for things we reference in online work and Copyright protects your work from being used incorrectly by others for profit. • Explain the Ethics of Hacking exploits weaknesses in a security system and there are white, black and gray hackers operating according to different ethical rules. • Communication systems or businesses apply risk management scenarios in their daily operations. • Hackers use cryptography in various scenarios thus it is important that symmetric and asymmetric Cryptography are used to secure data from hackers. • Settings and access for multiple users on a network must be established as part of a secure network. • Operating System Utilities are an essential part of a Network security system. • There are various methods for monitoring Networks. • Different systems have different vulnerabilities and it is important to understand how they may be attacked. • Understanding the difference between types of malware including: viruses, ransomware, worms, trojan horse, rootkits, keylogger, spyware, etc. allows for different methods for securing network access.
Duration/Credits:	Semester/ 0.5 credit
Course Materials/Resources:	Networking equipment and various computer hardware and software
FPS Course Academic Expectation(s):	EU: Exploring and Understanding CI: Conveying Ideas
Semester at a Glance (Units)	Unit 1: Ethics, Digital Citizenship and Computer Insecurity (3 weeks) Unit 2: Risk Management (3 weeks) Unit 3: Cryptography (3 weeks) Unit 4: Identity and Access Management (3 weeks) Unit 5: Network System Structure (3 weeks) Unit 6: Securing Devices and Individual systems (3 weeks)

Unit Number and Title:	Unit 1: Ethics, Digital Citizenship and Computer Insecurity
Duration:	3 weeks
Resource(s):	Computer Workstations and miscellaneous software or online resources.
Unit Overview:	This unit explores one's digital footprint and the necessary precautions people in today's digital connected world must take in order to protect themselves from harm.
Learning Goals	
Standard(s):	**CSTA Standards** 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks. (P7.2) 3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts. (P3.3) 3A-IC-29 Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users. (P7.2) 3A-IC-30 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics. (P7.3)
Essential Question(s):	● What necessary precautions must people in today's digital connected world take in order to protect themselves from harm?
Enduring Understanding(s):	● A digital footprint can last forever and negatively impact one's reputation. ● Cyberbullying is done by participants to anonymously take advantage of others. ● There are many things one can do to stay safe online ● Explain Information Literacy and affective search principles ● It is important to give proper Creative Credit for things we reference in online work and Copyright protects your work from being used incorrectly by others for profit. ● Explain the Ethics of Hacking exploits weaknesses in a security system and there are white, black and gray hackers operating according to different ethical rules.

Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● types of Hackers and hacking. ● artificial Intelligence and its uses. ● cyberbullying. **Skills:** (Students will be able to…) ● evaluate their own and others digital footprint. ● react to a cyber bullying scenarios. ● distinguish the type of hacker or the ethics of that hacker. ● identify and demonstrate appropriate use of artificial intelligence.

Unit Number and Title:	Unit 2: Risk Management
Duration:	3 weeks
Resource(s):	Computer Workstations
Unit Overview:	This unit explores risk, risk management, and risk assessment systems in the social and business structures of our world.
Learning Goals	
Standard(s):	**CSTA Standards** **CSTA Standards** 3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system. (P6.3) 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations. (P7.2))
Essential Question(s):	● How do risk, risk management, and risk assessment systems affect the social and business structures of our world?
Enduring Understanding(s):	● Communication systems or businesses apply risk management scenarios in their daily operations.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● types of Hackers and hacking. ● artificial Intelligence and its uses. ● cyberbullying. **Skills:** (Students will be able to…) ● explain risk as it relates to Communication systems and business. ● define risk management concepts and framework.

	• explain how risk is assessed.

Unit Number and Title:	Unit 3: Cryptography
Duration:	3 weeks
Resource(s):	Computer Workstations. Network Switches and routers, LAN network Server
Unit Overview:	Students will learn about cryptography algorithms and their basic characteristics, and learn how to implement public key infrastructure
Learning Goals	
Standard(s):	**CTSA Standards** *3A-AP-22 Design and develop computational artifacts working in team roles using collaborative tools. (P2.4)* *3A-DA-11 Create interactive data visualizations using software tools to help others better understand real world phenomena. (P4.4)*
Essential Question(s):	● Why must we use security systems for any time we are transferring or storing data?
Enduring Understanding(s):	● Hackers use cryptography in various scenarios thus it is important that symmetric and asymmetric Cryptography are used to secure data from hackers.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● symmetric Cryptography. ● asymmetric Cryptography. **Skills:** (Students will be able to…) ● define and create various types of cryptography. ● explain the difference between hashing algorithms. ● explain cryptographic attack strategies. ● determine attackable data.

	• understand attack scenarios.

Unit Number and Title:	Unit 4: Identity and Access Management
Duration:	3 weeks
Resource(s):	Computer Workstations
Unit Overview:	This unit explores access management practices and the concept of privilege in the security of sensitive information.
Standard(s):	**CompTIA Security+ objective:** ● 4.1 Compare and contrast identity and access management concepts ● 4.2 Given a scenario, install and configure identity and access services ● 4.3 Given a scenario, implement identity and access management controls ● 4.4 Given a scenario, differentiate common account management practices
Essential Question(s):	● Why is account and access management so important to network security?
Enduring Understanding(s):	● Settings and access for multiple users on a network must be established as part of a secure network.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● point to point authentication ● managing access on a network. **Skills:** (Students will be able to…) ● explain the meaning of Authentication, Authorisation, Accounting'. ● describe how Access and accounts are managed on networked systems. ● explain point-to-point authentication.

Unit Number and Title:	Unit 5: Network System Structure
Duration:	3 weeks
Resource(s):	Computer Workstations
Unit Overview:	This unit explores the importance of scanning and monitoring networks through common tools.
Standard(s):	**CTSA Standards** 3A-NI-04 Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing. (P4.1) 3A-AP-15 Justify the selection of specific control structures when tradeoffs involve implementation, readability, and program performance, and explain the benefits and drawbacks of choices made. (P5.2) 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations. (P7.2)
Essential Question(s):	● What vulnerabilities are there in networked systems?
Enduring Understanding(s):	● Operating System Utilities are an essential part of a Network security system. ● There are various methods for monitoring Networks.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● tools used to monitor networks. ● AI can be used to improve efficiency on a network. ● network scanners, scanning methods, targets, types and their purpose. **Skills:** (Students will be able to…) ● utilize operating system utilities. ● scan a network. ● monitor a network using applicable tools. ● identify ways AI can be used to improve security and efficiency on a network.

Unit Number and Title:	Unit 6: Securing Devices and Individual Systems
Duration:	3 weeks
Resource(s):	Computer workstations
Unit Overview:	In this unit, students will explore the different methods used for securing network access and thinking like an adversary, to understand how attacks are carried out.
Learning Goals	
Standard(s):	**CTSA Standards** 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks. (P7.2) 3A-CS-03 Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix errors. (P6.2) 3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system. (P6.3)
Essential Question(s):	● How does having a variety of system options and different vulnerabilities affect the cyber security industry?
Enduring Understanding(s):	● Different systems have different vulnerabilities and it is important to understand how they may be attacked. ● Understanding the difference between types of malware including: viruses, ransomware, worms, trojan horse, rootkits, keylogger, spyware, etc. allows for different methods for securing network access.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● attacks including; applications, operating systems, networks stacks, and drivers. **Skills:** (Students will be able to…)

	● identify vulnerabilities given relative system information. ● identify the proper protocol for security breaches. ● identify ways AI can be used to improve security and efficiency on an individual device.