Computer Engineering V: Cybersecurity and Hacker Defense

Course Information

Grade(s):	12
Discipline/Course:	Technology Education
Course Title:	Computer Engineering V: Cybersecurity and Hacker Defense
Prerequisite(s):	Computer Engineering IV: Networking and Troubleshooting *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, and what are the vulnerabilities? ● How do different elements of a connected network provide secure communications ranging from the smallest home LANs to an enterprise-level network? ● Why do organizations need to understand the ways attackers can gain access to their infrastructure? ● Why do organizations need to test infrastructure thoroughly for weaknesses and what are the response protocols? ● How can artificial intelligence (AI) be useful in computer security? ● How can artificial intelligence (AI) be harmful in computer security?
Course Enduring Understandings:	● The foundation of Cybersecurity is the CIA Triad: **C**onfidentiality, **I**ntegrity, and **A**vailability. ● CIA is the model security measure that should be guaranteed in every secure system.
Duration/Credits:	Full-Year/1 credit

Course Materials/Resources:	Networking equipment and various computer hardware and software
FPS Course Academic Expectation(s):	EU: Exploring and Understanding CI: Conveying Ideas
Year 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 7: LAN Setup and Security (3 weeks) Unit 8: Securing Wireless Networks (3 weeks) Unit 9: Secure protocols (3 weeks) Unit 10: Network Security Testing (3 weeks) Unit 11: Responding To Network Security Incidents (3 weeks) Unit 12: Coding for Networks (SQL and PHP) (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…) ● attacked 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.

Unit Number and Title:	Unit 7 - LAN Setup and Security
Duration:	3 Weeks
Resource(s):	Computer workstations, network switches and routers, LAN network Server
Unit Overview:	Students will learn the elements of different types of networks, and build upon this knowledge with learning what is required to provide secure communications within each type. (For networks ranging from home LANs to a complete enterprise-level network affect security.)
Learning Goals	
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-DA-10 Evaluate the tradeoffs in how data elements are organized and where data is stored. (P3.3)
Essential Question(s):	● How do different elements of a network provide secure communications ranging from the smallest home LANs to a complete enterprise-level network affect security?
Enduring Understanding(s):	● Through Switches and Routers and other security solutions for Local Area Networks and Virtual Private Network intrusion of the networks can be detected and prevented .
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● LAN - Local Area Network. ● VPN - Virtual Private Network. **Skills:** (Students will be able to…) ● set up a LAN network and its necessary hardwear. ● establish a security system for a LAN network.

Unit Number and Title:	Unit 8 - Securing Wireless Networks
Duration:	3 weeks
Resource(s):	Computer Workstations
Unit Overview:	Students will learn the roles of team members, working to protect a network, following system protocols, and implementing security measures.
Standard(s):	3A-NI-04 Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing. (P4.1) 3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system. (P6.3)
Essential Question(s):	● How do secure protocols used in TCP/IP networks provide security for Web applications covering both their attack vectors and the tools used to develop secure Web applications?
Enduring Understanding(s):	● Wireless networks are vulnerable to attack. ● A number of steps can be taken to secure wireless networks. ● Secure protocols used in TCP/IP networks provide security for Web applications.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● Wireless network attack protocols and defense. **Skills:** (Students will be able to…) ● set up a wireless network ● establish correct secure protocols for a network. ● given a scenario, defend a wireless network from an attack.

	● explain unique requirements of securing wireless networks. ● describe Protocols for wireless cryptography and authentication processes. ● describe different ways that wireless networks can be attacked/hacked. ● explain how to secure wireless networks against various attacking methods. ● explain how virtualization affects security. ● list environmental issues and solutions for securing data.

Unit Number and Title:	Unit 9 - Secure protocols
Duration:	3 weeks
Resource(s):	Computer workstations
Unit Overview:	Students will grow their troubleshooting strategies when defending a network, to ensure confidentiality, integrity, and availability are all present.
Learning Goals	
Standard(s):	CSTA 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):	● What considerations must be made in order to create functional and reliable communications between secure networks?
Enduring Understanding(s):	● It is important to know how web and E-mail applications may be attacked and how to secure them from attack.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● security protocols for given situations. ● secure internet protocols including DNSSEC, SNMP, SSH, FTP, SRTP. **Skills:** (Students will be able to…) ● select and implement the correct secure protocol for a given situation. ● set up a secure web application. ● defend a web application from an attack

Unit Number and Title:	**Unit 10- Network Security Testing**
Duration:	3 weeks
Resource(s):	Computer workstations
Unit Overview:	Students will explore the actions that are taken after security assessments are completed, how this information is constructed, and next steps to protect network security.
Learning Goals	
Standard(s):	3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system. (P6.3) 3A-IC-27 Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields. (P2.4) 3A-IC-28 Explain the beneficial and harmful effects that intellectual property laws can have on innovation. (P7.3) 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):	● Why do organizations not only need to understand the ways attackers can gain access to their infrastructure, but also need to test infrastructure thoroughly for any weakness?
Enduring Understanding(s):	● It is important to identify and assess the Vulnerability of a network to protect against attacks through weak points in a system.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● different hardware, configurations, and applications. ● the impact social engineering has on securing systems. ● security assessments and risk calculations.

	Skills: (Students will be able to…): ● distinguish between pieces of hardware. ● identify security risks of a given hardwear piece or application. ● calculate the risk based on a given scenario and set of parameters.

Unit Number and Title:	Unit 11 - Responding To Network Security Incidents
Duration:	3 weeks
Resource(s):	Computer workstations
Unit Overview:	Students will focus on building a strong knowledge base in both hardware and software to allow them to respond to security incidents effectively.
Standard(s):	3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system. (P6.3) 3A-CS-03 Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix errors. (P6.2)
Essential Question(s):	● How do we respond to incidents ranging from the minor (like a system crash) to the major (natural disaster wiping out the company HQ)
Enduring Understanding(s):	● Digital forensic analysis can result in conclusions of possible hack methods and potential solutions that can be used to respond to an attack. ● Risk management practices can be incorporated by businesses into their daily operations to protect against possible catastrophic attacks on the computer network.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● Digital forensic techniques. **Skills:** (Students will be able to…) ● Employ digital forensic techniques to a given scenario. ● Provide security advice based on security needs of a given business through an understanding. of their network hardware, weaknesses and vulnerabilities.

Unit Number and Title:	Unit 12 - Coding for Networks (SQL and PHP)
Duration:	3 weeks
Resource(s):	Computer workstations
Unit Overview:	In this unit, students explore the importance of accessing and manipulating databases for cyber security and networks using Python.

Standard(s):	3A-AP-17 Decompose problems into smaller components through systematic analysis, using constructs such as procedures, modules, and/or objects. (P3.2) 3A-AP-18 Create artifacts by using procedures within a program, combinations of data and procedures, or independent but interrelated programs. (P5.2) 3A-AP-19 Systematically design and develop programs for broad audiences by incorporating feedback from users. (P5.1) 3A-AP-22 Design and develop computational artifacts working in team roles using collaborative tools. (P2.4) 3A-AP-23 Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs. (P7.2)
Essential Question(s):	● Why should a cybersecurity technician be proficient in coding languages such as SQL and PHP?
Enduring Understanding(s):	● Networks are structured and manipulated using various computer codes to perform tasks.
Learning Goal(s): *Students will be able to use their learning to:* (Content/ Skills)	**Content:** (Students will know…) ● SQL and PHP **Skills:** (Students will be able to…) ● manipulate databases with SQL and PHP commands.