



Computer Engineering V: Cybersecurity and Hacker Defense

Second Semester

Course Information

Grade(s):	12
Discipline/Course:	Technology Education
Course Title:	Computer Engineering V: Cybersecurity and Hacker Defense, Semester II
Prerequisite(s):	Computer Engineering IV: Networking and Troubleshooting (Full Year) <i>or</i> Computer Engineering IV: Networking and Troubleshooting (Semester) with teacher's permission, <i>or</i> Computer Engineering V: Cybersecurity and Hacker Defense (Semester) with teacher's permission
Course Description: <i>Program of Studies</i>	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:	<ul style="list-style-type: none"> ● How do different elements of a network provide secure communications ranging from the smallest home LANs to a complete enterprise-level network affect security? ● 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? ● What considerations must be made in order to create functional and reliable communications between secure networks? ● 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? ● How do we respond to incidents ranging from the minor (like a system crash) to the major (natural disaster wiping out the company HQ) ● Why should a cybersecurity technician be proficient in coding languages such as SQL and PHP?

Course Enduring Understandings:	<ul style="list-style-type: none"> ● 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. ● 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. ● It is important to know how web and E-mail applications may be attacked and how to secure them from attack. ● It is important to identify and assess the Vulnerability of a network to protect against attacks through weak points in a system. ● Networks are structured and manipulated using various computer codes to perform tasks.
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: LAN Setup and Security (3 weeks) Unit 2: Securing Wireless Networks (3 weeks) Unit 3: Secure protocols (3 weeks) Unit 4: Network Security Testing (3 weeks) Unit 5: Responding To Network Security Incidents (3 weeks) Unit 6: Coding for Networks (SQL and PHP) (3 weeks)

Unit Number and Title:	Unit 1: 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):	<ul style="list-style-type: none"> 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):	<ul style="list-style-type: none"> 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): <i>Students will be able to use their learning to:</i> (Content/ Skills)	Content: (Students will know...) <ul style="list-style-type: none"> LAN - Local Area Network. VPN - Virtual Private Network. Skills: (Students will be able to...) <ul style="list-style-type: none"> set up a LAN network and its necessary hardware. establish a security system for a LAN network.

Unit Number and Title:	Unit 2: 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):	<ul style="list-style-type: none"> 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):	<ul style="list-style-type: none"> 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): <i>Students will be able to use their learning to:</i> (Content/ Skills)	<p>Content: (Students will know...)</p> <ul style="list-style-type: none"> wireless network attack protocols and defense. <p>Skills: (Students will be able to...)</p> <ul style="list-style-type: none"> 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.

- | | |
|--|--|
| | <ul style="list-style-type: none">● 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 3: 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):	<ul style="list-style-type: none"> • What considerations must be made in order to create functional and reliable communications between secure networks?
Enduring Understanding(s):	<ul style="list-style-type: none"> • It is important to know how web and E-mail applications may be attacked and how to secure them from attack.
Learning Goal(s): <i>Students will be able to use their learning to:</i> (Content/ Skills)	<p>Content: (Students will know...)</p> <ul style="list-style-type: none"> • security protocols for given situations. • secure internet protocols including DNSSEC, SNMP, SSH, FTP, SRTP. <p>Skills: (Students will be able to...)</p> <ul style="list-style-type: none"> • 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 4: 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):	<p>3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system. (P6.3)</p> <p>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)</p> <p>3A-IC-28 Explain the beneficial and harmful effects that intellectual property laws can have on innovation. (P7.3)</p> <p>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)</p> <p>3A-IC-30 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics. (P7.3)</p>
Essential Question(s):	<ul style="list-style-type: none"> 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):	<ul style="list-style-type: none"> 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): <i>Students will be able to use their learning to:</i> (Content/ Skills)	Content: (Students will know...) <ul style="list-style-type: none"> 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 hardware piece or application.
- calculate the risk based on a given scenario and set of parameters.

Unit Number and Title:	Unit 5: 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):	<ul style="list-style-type: none"> • 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):	<ul style="list-style-type: none"> • 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): <i>Students will be able to use their learning to:</i> (Content/ Skills)	<p>Content: (Students will know...)</p> <ul style="list-style-type: none"> • digital forensic techniques. <p>Skills: (Students will be able to...)</p> <ul style="list-style-type: none"> • 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 6: 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):	<p>3A-AP-17 Decompose problems into smaller components through systematic analysis, using constructs such as procedures, modules, and/or objects. (P3.2)</p> <p>3A-AP-18 Create artifacts by using procedures within a program, combinations of data and procedures, or independent but interrelated programs. (P5.2)</p> <p>3A-AP-19 Systematically design and develop programs for broad audiences by incorporating feedback from users. (P5.1)</p> <p>3A-AP-22 Design and develop computational artifacts working in team roles using collaborative tools. (P2.4)</p> <p>3A-AP-23 Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs. (P7.2)</p>
Essential Question(s):	<ul style="list-style-type: none"> • Why should a cybersecurity technician be proficient in coding languages such as SQL and PHP?
Enduring Understanding(s):	<ul style="list-style-type: none"> • Networks are structured and manipulated using various computer codes to perform tasks.
Learning Goal(s): <i>Students will be able to use their learning to:</i> (Content/ Skills)	<p>Content: (Students will know...)</p> <ul style="list-style-type: none"> • SQL and PHP. <p>Skills: (Students will be able to...)</p> <ul style="list-style-type: none"> • manipulate databases with SQL and PHP commands.

