Chino Valley Unified School District
High School Course Description

A. CONTACTS	
1. School/District Information:	School/District: Chino Valley Unified School District Street Address: 5130 Riverside Drive Phone: (909) 628-1201 Website: chino.k12.ca.us
2. Course Contact:	Teacher Contact: Office of Secondary Curriculum Position/Title: Director of Secondary Curriculum Site: District Office Phone: (909) 628-1201 X1630
B. COVER PAGE - COURSE ID	
1. Course Title:	Advanced Cybersecurity Honors
2. Transcript Title/Abbreviation:	Adv Cybersec H
3. Transcript Course Code/Number:	5E87
4. Seeking Honors Distinction:	Yes
5. Subject Area/Category:	Meets UC/CSU "G" elective credit
6. Grade Level(s):	11th; 12th
7. Unit Value:	5 credits per semester; 10 credits total
8. Course Previously Approved by UC:	Yes
9. Classified as a Career Technical Education Course:	No
10. Modeled after an UC-approved course:	No
11. Repeatable for Credit:	No
12. Date of Board Approval:	May 2, 2024
13. Brief Course Description: Advanced Cybersecurity introduces the core security concepts and skills needed to monitor, detect, analyze, and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. Learners in this course are exposed to all the foundational knowledge required to detect, analyze, and escalate basic cybersecurity threats using common open-source tools, such as the Cyber Kill Chain. This course aligns with and prepares students for the Cisco Certified CyberOps Associate (CBROPS) certification assessment. In order to assist with learning and demonstrating mastery of content, students will, throughout this course, be engaging in close reading and annotation of complex text, collaborating with peers to complete research and virtual machine tasks, and completing informal and formal writing assignments.	
14. Prerequisites:	Cybersecurity Honors
15. Context for Course: Aligned with the California Common Core State Standards (CCSS) and the State of California Computer Science Standards, Advanced Cybersecurity Honors is designed to develop student skills in advanced cybersecurity and threat analysis topics. Students will explore the key principles of cybersecurity and networking defense, such as cybercrimes, cyber laws and ethics, Windows and Linux operating systems, networking, and security technologies and protocols. In addition to developing core cybersecurity and computer science competencies, the course also includes opportunities for students to analyze complex technical texts and compose short and sustained research projects to answer cybersecurity questions.	
16. History of Course Development: Advanced Cyber Security Honors is the second course in the Cybersecurity: Information and Communication Technology pathway. This course builds upon the course work of Cybersecurity Honors and prepares students for the Cisco Certified CyberOps Associate (CBROPS) certification assessment.	
17. Textbooks:	N/A
18. Supplemental Instructional Materials:	CISCO Network Academy https://www.netacad.com/

C. COURSE CONTENT

1. Course Purpose:

This course is the second and final course in a Cybersecurity sequence designed for students in the Cybersecurity: Information and Communication Technology pathway at the Biomedical Science and Technology Academy (BST).

2. Course Outline:

UNIT 1: CYBER LAWS AND ETHICS

Unit 1 Summary

Students will explore current legal case studies pertaining to violations of cybersecurity ethics and compliance. They will research various types of cybercrimes, including criminal activities targeting computers and networks, and/or networked devices, as well as "cyber-enabled" crimes – criminal activities carried out via the Internet or aided by computer technology, such as using social media as a platform to bully others and identity theft. Students will examine legal and ethical issues in cybersecurity, learning how the laws that govern fair use and copyright protect privacy in the 21st century, and how criminal evidentiary laws dictate what information stored on a computer can be used as evidence. They analyze the Cyber Security Act of 2015 and the role the Federal Cybersecurity Mandates have in the practices, policies, and procedures required in public and private industries.

Unit 1 Learning Goals

- Describe various types of cybercrimes
- Explain fair use and copyright laws
- Explain what evidence can be used for cybercrimes
- Describe different Cyber Security laws and mandates that protect against cybercrimes

UNIT 2: DANGERS AND FIGHTERS

Unit 2 Summary

This unit begins with outlining different cyber-attacks in history and exploring the question “What are the dangers of cyber-attacks?”. Students will learn and be able to compare the different types of threat actors and threat impacts. Students will also learn about how Internet of Things (IOT) devices are under attack and how they impact our daily living. Students will investigate what kinds of information threat actors can access through IOT devices. Lastly, students will learn about how to fight against cyber-attacks, specifically the Security Operations Center. Students will conclude with researching different cybersecurity jobs that protect against cyber dangers and the adequate education for those roles.

Unit 2 Learning Goals

- Outline features of cybersecurity incidents
- Explain the motivations of the threat actors behind specific security incidents
- Explain the potential impact of network security attacks
- Explain the mission of the security operations center
- Describe resources available to prepare for a career in cybersecurity operations

UNIT 3: WINDOWS AND LINUX

Unit 3 Summary

In this unit Windows and Linux, students begin with exploring the security features of the Windows Operating System. Students will learn about the history and various updates the Windows Operating System has undergone as it has improved throughout the years. Students will be able to describe the different commands, processes, and services Windows offers and utilizes to be able to access network along with provide security. Students will then be able to compare this with Linux and describe each’s advantages. Students then learn how to work with the Linux Shell, Linux file system, and Linux commands to change text files, manipulate security log files, manage permissions, and to detect malware on the host.

Unit 3 Learning Goals

- Describe the history of the Windows Operating System
- Explain the architecture of Windows and its operation
- Explain how to configure and monitor Windows
- Explain how Windows can be kept secure
- Explain why Linux skills are essential for network security monitoring and investigation
- Use the Linux shell to manipulate text files
- Explain how client-server networks function
- Explain how a Linux administrator locates and manipulates security log files
- Manage the Linux file system and permissions
- Explain the basic components of the Linux GUI (Graphical User Interface)
- Use tools to detect malware on a Linux host

UNIT 4: NETWORK, INTERNET, AND ETHERNET PROTOCOLS

Unit 4 Summary

Network, Internet, and Ethernet Protocols introduce students to the concept of how protocols such as Ethernet and IP protocols allow network operations. Students learn to trace an internet pathway to networks, being able to classify the type of network. Students then learn to describe the different network protocols (HTTP, TCP, IP...) that allow for computers to communicate on networks. The next section (Internet and Ethernet Protocols) outlines how IP addresses (IPv4 and IPv6), default gateways, and Ethernet support network communication. Students examine exactly how IPv4 and IPv6 addresses work and their different classes and blocks. Students also learn how to use different commands like netstat to display and analyze routing tables and to complete networking diagrams.

Unit 4 Learning Goals

- Explain the basic operations of data networked communications
- Explain how protocols enable network operations
- Explain how data encapsulation allows data to be transported across the network
- Explain how Ethernet supports network communication
- Explain how the IPv4 protocol supports network communications
- Explain how IP addresses enable network communication
- Explain the types of IPv4 addresses that enable network communication
- Explain how the default gateway enables network communication
- Explain how the IPv6 protocol supports network communications

UNIT 5: NETWORKING SECURITY, CONNECTIVITY, AND FUNCTIONALITY

Unit 5 Summary

In this unit, students will start out exploring how to verify connectivity with different tools such as ping and traceroute. Students will practice utilizing these different commands on Packet Tracers and Virtual Machines. Further, students will break down exactly how networking can happen by learning about IP addresses, MAC addresses, and ARPs. Students will practice identifying IP addresses and MAC addresses utilizing ARP tables and different commands. Lastly, this unit explores the idea of network functionality, focusing on how the transport layer allows network communication. Students will explain design considerations when implementing IPv6 and IPv4 in different types of networks.

Unit 5 Learning Goals

- Explain how ICMP is used to test network connectivity
- Use Windows tools, ping, and traceroute to verify network connectivity
- Compare the roles of the MAC address and the IP address
- Analyze ARP by examining Ethernet frames
- Explain how ARP requests impact network and host performance
- Explain how transport layer protocols support network communication
- Explain how the transport layer establishes communication sessions
- Explain how the transport layer establishes reliable communications

UNIT 6: NETWORK SERVICES, DEVICES, AND SECURITY

Unit 6 Summary

In this unit, students will learn to explain how network services enable network functionality. Students will compare how DHCP, DNS, NAT, file transfer, email, and HTTP services enable network functionality. Next, students explore how network devices enable wired and wireless network communication. Students explain the two primary functions of routers and practice building network diagrams (LANS, VLANS) with routers. Furthermore, students explain how devices and services are used to enhance network security. Students compare the different common security architectures and the security devices. Lastly, students debate which security service (IDS, SPAN, Netflow, SNMP, AAA, Syslog...) is the most effective or appropriate under different circumstances.

Unit 6 Learning Goals

- Explain how DHCP services enable network functionality
- Explain how DNS services enable network functionality
- Explain how NAT services enable network functionality
- Explain how file transfer services enable network functionality
- Explain how email services enable network functionality
- Explain how HTTP services enable network functionality
- Explain how network devices enable network communication
- Explain how wireless devices enable network communication
- Explain how network designs influence the flow of traffic through the network
- Explain how specialized devices are used to enhance network security
- Explain how network services enhance network security

UNIT 7: ATTACKS AND THREATS

Unit 7 Summary

This unit will have students distinguish and identify common network attacks and system security threats with how to determine an attack event has occurred on a Windows network. Students will reverse track and identify an attack event's point of origin along with characteristics of a Denial-of-Service attack (e.g. methods used in Smurf, Ping of Death, SYN flood). Lastly, students explain key differences between Viruses, Worms, Trojans, Rootkits, and Bots; Phishing, Port-Redirection, Man-in-the-Middle, Brute-Force and Rogue Access Points.

Unit 7 Learning Goals

- Explain how network threats have evolved
- Describe the various types of attack tools used by Threat Actors
- Describe types of malwares
- Explain reconnaissance, access, and social engineering attacks
- Explain denial of service, buffer overflow, and evasion attacks

UNIT 8: NETWORK OPERATIONS AND NETWORK ATTACKS

Unit 8 Summary

In this unit. Students will explain network traffic monitoring by trying out the different tools that are used in the industry. These tools (IDS, packet analyzers, SNMP, Netflow...) will be practiced through different labs and Packet Tracers. Next, students explain how TCP/IP vulnerabilities enable network attacks. Students will analyze how IP headers allow for Spoofing and Reflection attacks to occur. Lastly, students start to explain how common network applications and services are vulnerable to attack. Students compare different types of attacks such as DNS open resolver, DNS Stealth, DNS Domain Shadowing, and DNS Tunneling.

Unit 8 Learning Goals

- Explain the importance of network monitoring
- Explain how network monitoring is conducted
- Explain the IPv4 and IPv6 header structure
- Explain how IP vulnerabilities enable network attacks
- Explain how TCP and UDP vulnerabilities enable network attacks
- Explain IP service vulnerabilities
- Explain how network application vulnerabilities enable network attacks

UNIT 9: DEFENSE AND ACCESS

Unit 9 Summary

This unit starts with a system audit including event logs, ports, processes, services, variables, paths, and file properties and continuing with common areas targeted by virus attacks and their characteristic signs of intrusion (e.g. registry, services, dlls). Administering the system firewall access control and identifying common port services used (e.g. email, FTP, etc.) along with configuring a router for typical defense measures and wireless security settings (e.g. DHCP, WPK, disable ICMP, etc.) How to render a network invisible to an intruder using custom subnets (i.e. network enumeration) and different ways to use the last known good control set to quickly recover from an attack event. How a multi-boot system can be used to recover and launch a countermeasure to a recent attack.

Unit 9 Learning Goals

- Explain how the defense-in-depth strategy is used to protect networks
- Explain security policies, regulations, and standards
- Explain how access control protects network data
- Explain how AAA is used to control network access

UNIT 10: THREAT INTELLIGENCE AND CRYPTOGRAPHY

Unit 10 Summary

Protecting data as it traverses a network or while it's stored on a computer is one of the most important jobs of a network security professional. Students learn about how companies and private individuals don't want others to view confidential documents and files. In this unit, students examine the various cryptography technologies that security professionals use to protect a company's data. Students see how information can be converted into an unreadable format and how only those with the correct key or "decoder" can read the message. Students also look at various cryptography attacks and some of the tools used to conduct these attacks.

Unit 10 Learning Goals

- Describe information sources used to communicate emerging network security threats
- Describe various threat intelligence services
- Explain the role of cryptography in ensuring the integrity and authenticity data
- Explain how cryptographic approaches enhance data confidentiality
- Explain public key cryptography
- Explain how the public key infrastructure functions
- Explain how the use of cryptography affects cybersecurity operations

UNIT 11: ENDPOINT PROTECTION AND VULNERABILITY

Unit 11 Summary

In this unit, students will explore how a malware analysis website generates a malware analysis report. Students will research different Antivirus and Antimalware software to discover how they detect and mitigate viruses and malware. Further, students explain how endpoint vulnerabilities are assessed and managed. Students will utilize the Common Vulnerability Scoring System to rate the risks of different given vulnerabilities. Finally, students will discuss different risk management techniques and how to decide on different security controls for different organizations/occasions.

Unit 11 Learning Goals

- Explain methods of mitigating malware
- Explain host based IPS/IDS log entries
- Explain how sandboxes are used to analyze malware
- Explain the value of network and server profiling
- Explain how CVSS reports are used to describe security vulnerabilities
- Explain how secure device management techniques are used to protect data and assets
- Explain how information security management systems are used to protect assets

UNIT 12: SECURITY TECHNOLOGIES AND PROTOCOLS

Unit 12 Summary

In this unit, students will explain how security technologies affect security monitoring. Students learn about how Syslog sends log entries and helps make security monitoring practical. Students also compare HTTP versus HTTPS by looking at their vulnerabilities and deciding which is more secure. Lastly, students explore encryption, NAT, PAT, and load balancing to discover how they complicate security monitoring.

Unit 12 Learning Goals

- Explain the behavior of common network protocols in the context of security monitoring
- Explain how security technologies affect the ability to monitor common network protocols
- Compare the different security technologies advantages and disadvantages
- Analyze which security technology is most appropriate under different circumstances

UNIT 13: NETWORK SECURITY - ALERTS, LOGS, AND DATA

Unit 13 Summary

This unit starts with students explaining the types of network security data used in security monitoring. Students explore what makes up session data (IP addresses, port numbers, etc.) and how that data can be analyzed by cyber specialists. Next, students explain and explore the process of evaluating alerts. Students practice classifying alerts as True Positive or False Positive, along with practicing identifying situations that are True Negative and False Negative. Last, students interpret data to determine the source of a given alert. Students practice using Sguil, Kibana, and Wireshark to investigate different attacks.

Unit 13 Learning Goals

- Describe the types of data used in security monitoring
- Describe the elements of an end device log file
- Describe the elements of a network device log file
- Identify the structure of alerts
- Explain how alerts are classified
- Explain how data is prepared for use in Network Security Monitoring (NSM) system
- Use Security Onion tools to investigate network security events
- Describe network monitoring tools that enhance workflow management

UNIT 14: DIGITAL FORENSICS AND INCIDENT ANALYSIS AND RESPONSE

Unit 14 Summary

In this unit, students learn what types of digital and physical evidence are essential to acquire at a cybercrime scene. Students get hands-on experience in identifying and cataloging anomalous network packets; malware analysis; honeypots and host-based intrusion detection systems; recovering and analyzing volatile evidence; forensic imaging over a network; and identifying and analyzing evidence of server intrusion. They complete simulated affidavits for search warrants, process crime scenes, collect and analyze evidence, and prepare testimony via utilization of digital and physical forensic tools. Students explore the difference between "live forensics resources" and "saved resources" to ensure the protection and integrity of digital and physical evidence.

Unit 14 Learning Goals

- Explain the role of digital forensic processes
- Identify the steps in the Cyber Kill Chain
- Classify an intrusion event using the Diamond Model
- Apply the NIST 800-61r2 incident handling procedures to a given incident scenario
- Analyze evidence after a cyber-attack

3. Key Assignments:

UNIT 1: CYBER LAWS AND ETHICS

The class will be split into two teams to debate a cybersecurity issue with questionable ethics. One team will argue in favor of the issue; the other against it. Team members will collaborate to investigate and research the question, formulate a claim, and support it with evidence. They will also need to anticipate possible challenges and have evidence ready to refute them. Students will need to integrate multiple pieces of information into a strong and cohesive argument that considers all sides of the issue, resolves contradictions when possible, and determine what additional information or research is required to deepen the investigation. Within this assignment, students will:

- Utilize critical thinking to make sense of problems and persevere in solving them
- Model integrity, ethical leadership, and effective management
- Work productively in teams while integrating cultural/global competence
- Conduct research to solve a problem unique to the Information Technology and Systems industry using critical and creative thinking, logical reasoning, analysis, and problem-solving
- Initiate and participate effectively in collaborative discussions, building on others' ideas and expressing their own clearly
- Research - create and present how laws and ethics shape policy regarding computer access and security protocols. Students must draw evidence from information texts to support their analysis

UNIT 2: DANGERS AND FIGHTERS

The class will be divided into groups and assigned different Cybersecurity Cases and will have to analyze and answer different questions regarding the cases. They will research the vulnerabilities that were taken advantage of for their case. Based on their case, they will create a written proposal on how the organization could have prevented this attack. Groups will then present their case and proposal to the class, highlighting how this attack could have been defended against. Within this assignment, students will:

- Conduct research on cybersecurity incidents
- Collaborate with team members
- Synthesize relevant information
- Create a concise and well-evidenced proposal

UNIT 3: WINDOWS AND LINUX
In this lab, students will use administrative tools to monitor and manage system resources for the Windows Operating System. After completing various tasks for the Windows Operating System (such as Windows Registry, PowerShell, and Task Manager, students will explore Linux tools to manage files and system resources. After completing these various tasks for the Linux Operating System (such as Linux Shell, Command Line, and Linux filesystems), students will compare the two different operating systems. Students will compose a short essay comparing the different operating systems' commands, processes, security, and system resources.

UNIT 4: NETWORK, INTERNET, AND ETHERNET PROTOCOLS
Students will track and identify a "rogue" laptop that keeps changing names and IP addresses across multiple domains (e.g. scanner, arp, nbtstat, etc.). After tracking and identifying, students will summarize how they were able to track the rogue laptop. Students will also identify a "stolen" laptop on the Internet and trace it to its last known latitude and longitude (e.g. ArcExplorer, Google Earth, tracert, finger).

UNIT 5: NETWORKING SECURITY, CONNECTIVITY, AND FUNCTIONALITY
Students will complete a Packet Tracer assignment where the students have to verify IPv4 and IPv6 addressing configuration, along with test connectivity with different commands such as Ping and Tracert on a given network. After this, students must analyze and solve the networking issue if there is any resulting from the various connectivity tests. Students then compose a written response on how they found the issue in the topology and how they figured out how to resolve the error.

UNIT 6: NETWORK SERVICES, DEVICES, AND SECURITY
Students will be tasked with creating a logical topology for a medium-sized business. Students will have to create a proposal for this business to choose their design and layout. In their layout, they will have to consider LANs, WANs, the Three-Layer Network Design Model, firewalls, DMZ, IPS, ACL, routers, and more. In their proposal, they will have to explain why their design is the most effective and why it should be chosen. Students will present their designs and proposals to the class through making a PowerPoint/Slideshow.

UNIT 7: ATTACKS AND THREATS
Students will create an application capable of sending/receiving remote messages and files. They will use programming to create a network scanner to graphically display computers that are on or off. They will additionally scan TCP and UDP ports for real-time system intrusion and identify the intruder's MAC address (i.e. netstat, arp, NBTstat).

UNIT 8: NETWORK OPERATIONS AND NETWORK ATTACKS
Each group will be assigned a different type of DNS attack to research and present on. Students will be tasked to find a real-life example of their type of attack and write a written report explaining how that attack happened and what information it was able to steal. Lastly, in the written report, the group will have to create a solution or a way of preventing that attack from happening. On top of that, students will create a simulation of their attack to present to the class, exemplifying exactly how that attack takes place.

UNIT 9: DEFENSE AND ACCESS

Students explore examples of common cybersecurity problems. Students will simulate, design, and implement unique cybersecurity challenges in virtual images (which are simulated operating systems played on a virtual machine player). A different challenge will be chosen for each topic activity; challenges include: Access control and settings; Insecure services; Policy violations; File sharing and permissions; Malware; Updates: Operating System; Updates: Firewall; Updates: Other. Students will maintain and harden critical services, fix vulnerabilities, remove malware, and answer forensics questions. Each lab will take place on a different operating system virtual machine image. Virtual machine images will include Windows 8.1, Windows 10, Windows Server 2008, and Windows Server 2016, Ubuntu 14, Ubuntu 16, Debian 7, and others. Through these projects, students learn to find and fix security vulnerabilities in virtual operating systems; and apply, modify, and construct solutions to the discovery and remediation of vulnerabilities. Students also gain a deeper understanding and appreciation of fully securing all forms of electronic devices.

UNIT 10: THREAT INTELLIGENCE AND CRYPTOGRAPHY

Case 12-1: Determining Possible Vulnerabilities of Microsoft CA Root Server

In conducting security testing on the K. J. Williams network, you have identified that the company configured one of its Windows Server 2003 computers as an Enterprise root CAR server. You have also determined that Ronnie Jones, the administrator of the CA server, selected SHA-1 as the default hashing algorithm for creating digital signatures. Based on the preceding information, write a one-page report explaining possible vulnerabilities on the CA root server caused by the SHA-1 exploit. The report should cite any articles written about the SHA-1 vulnerability and include any recommendations from Microsoft about its use of theSHA-1 algorithm in its software applications.

Case 12-2: Exploring Moral Versus Legal Issues

After conducting the research for Case 12-1, you have gathered a lot of background on the release of information as it pertains to encryption algorithms. Articles on vulnerabilities of SHa-1, MD4 and MD5 abound. The proliferation of computer programs that break DVD encryption codes and the recent imprisonment of an attacker who broke Japan's encryption method for blocking certain images from pornographic movies have raised many questions on what is moral or legal in releasing information that exposes the algorithm used to encrypt data. Based on the preceding information, write a two-page report that addresses the moral and legal issues for the release of software or programmable code that breaks encryption algorithms. Your paper should also answer these questions:

- If a person can break the encryption of a particular algorithm, should they be allowed to post the findings on the Internet?
- Do you think the reporters of the DVD (DeCSS) crack were exercising their First Amendment rights when including the source code that breaks the DVD encryption key in an article? What about the source code being displayed on a T-shirt?
- As a security professional, do you think you have to abide by a higher standard when it comes to sharing or disseminating source code that breaks encryption algorithms? Explain.

UNIT 11: ENDPOINT PROTECTION AND VULNERABILITY

Students will research the NIST Cybersecurity Framework and analyze how it helps prevent cybersecurity attacks. Each group will be given a different core function in the NIST Cybersecurity Framework. Each group will have to complete a written report on their core function and how it manages and reduces cybersecurity risk. In their written report, they will have to connect prior strategies for defense and awareness they have learned for their assigned function. They will have to explain why those prior strategies connect to the core function and why it is necessary for companies to do.

UNIT 12: SECURITY TECHNOLOGIES AND PROTOCOLS
Students will be given a task that requires them to choose a security technology and analyze how it affects society in various ways. Students will have to complete a written report about their security technology, focusing on how that technology affects security monitoring. Students will have to conclude how their technology is helpful, but also include the vulnerabilities and weaknesses of their technology. This written report should be treated as an analysis review of the security technology they chose that would be published on a technology review website.

UNIT 13: NETWORK SECURITY - ALERTS, LOGS, AND DATA
Students will utilize Security Onion tools (Sguil, Kibana, and Wireshark) to investigate an exploit. From these tools, students must analyze what the exploit is and how it occurred. Students will then have to create a solution to the attack they identified from the analysis. Throughout this, students are answering short lab questions to summarize and analyze the alerts. This lab is based on an exercise from the website malware-traffic-analysis.net which is an excellent resource for learning how to analyze network and host attacks.

UNIT 14: DIGITAL FORENSICS AND INCIDENT ANALYSIS AND RESPONSE
Analyze digital forensic data systems, forensic software, and adhere to legal compliance in documenting digital evidence. Develop the topic thoroughly by selecting the most significant and relevant facts, extended definitions, concrete details, and other information specific to the task.

- Essay: Present information, findings, and supporting evidence (reflective of investigation) conveying a clear and distinct claim. Students will submit word (350 minimum) essay in (APA format)
- PowerPoint/Prezi Presentation or other digital method: Make strategic use of digital media (e.g., textual, graphical, audio, visual, and interactive elements) in presentation to enhance understanding of findings, reasoning, and evidence and to add
- Law/Legal Classroom Presentation & Lab: Present case to real legal/law professionals to validate students' findings and case presentation

FINAL EXAM DETAILS
Multiple Choice Exam: 60 questions modeled after the CyberOps Associate certification test to help students prepare to take the CyberOps Associate certification test.

Written Report: Students will write a written report (3-5 pages) from the following topic questions:

- Considering the importance of cybersecurity, what are some best practices that everyone must follow in both their personal and professional lives to ensure safety from cyber-attacks? Why?
- Research some recent cyber-attacks and how the organizations or people affected dealt with the aftermath of the attack (for example, what was the response plan? When were the victims notified? Was the hacker/attacker caught? How was the attack contained/stopped? What changes were made after the incident to prevent such an incident from occurring again?) If mishandled, what would have you done differently? If dealt with appropriately, what did they do correctly?

Performance Task: In teams of 4, students will be given a set of virtual images that represent operating systems and are tasked with finding cyber security vulnerabilities within the images and hardening the system while maintaining critical services and infrastructure. Students will have to make the system on their virtual image secure and fix any vulnerabilities that are present. These images will include Windows, Linux, and Ubuntu.

4. Instructional Methods and/or Strategies:

APB (Activity, Project, and Problem-based) Instructional Design centers on hands-on, real-world activities, projects, and problems that help students understand how the knowledge and skills they develop in the classroom may be applied to everyday life. The instructional methods and strategies utilized provide students with unique opportunities to work collaboratively, identify problems, apply what they know, persevere through challenges, find unique solutions, and lead their own learning. The APB approach scaffolds student learning through structured activities and projects that empower students to become independent in the classroom and help them build skill sets to apply to real-world and open-ended design problems.

- Four Corners discussions (Agree, Strongly Agree, Disagree, Strongly Disagree)
- Data collection, interpretation, and predictions
- Jig Saw research projects (students or student groups research different aspects of a topic and report their learning back to the whole class)
- Computer based research projects: individual students or collaborative group research
- Evidence based data interpretation (Claim, Evidence and Reasoning writing research projects)
- Student centered and created activities

5. Assessment Including Methods and/or Tools:

The evaluation of student progress and evaluation will be based on the following criteria outlined in Board Policy:

- Assessments: 60-75% of the final grade
- Assignments and class discussions: 25-40% of the final grade

UNITS WITH STANDARDS CORRELATIONS

UNIT 1 – CYBER LAWS AND ETHICS

CA Computer Science Standards

- 9-12.IC.26: Study, discuss, and think critically about the potential impacts and implications of emerging technologies on larger social, economic, and political structures, with evidence from credible sources
- 9-12.IC.30: Evaluate the social and economic implications of privacy in the context of safety, law, or ethics

CA Common Core State Standards

- CCSS.ELA-LITERACY.RST.1: Cite specific textual evidence to support analysis of science and technical texts, attending to important distinctions the author makes and to any gaps or inconsistencies in the account
- CCSS.ELA-LITERACY.RST.2: Determine the central ideas or conclusions of a text; summarize complex concepts, processes, or information presented in a text by paraphrasing them in simpler but still accurate terms
- CCSS.ELA-LITERACY.RST.7: Integrate and evaluate multiple sources of information presented in diverse formats and media (e.g., quantitative data, video, multimedia) in order to address a question or solve a problem
- CCSS.ELA-LITERACY.RST.8: Evaluate the hypotheses, data, analysis, and conclusions in a science or technical text, verifying the data when possible and corroborating or challenging conclusions with other sources of information
- CCSS.ELA-LITERACY.RST.9: Synthesize information from a range of sources (e.g., texts, experiments, simulations) into a coherent understanding of a process, phenomenon, or concept, resolving conflicting information when possible

UNIT 2 – DANGERS AND FIGHTERS

CA Computer Science Standards

- 9-12.NI.6 Compare and contrast security measures to address various security threats

CA Common Core State Standards

- CCSS.ELA-LITERACT.WHST.1: Write arguments focused on discipline-specific content
- CCSS.ELA-LITERACT.WHST.4: Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience

UNIT 3 – WINDOWS AND LINUX

CA Computer Science Standards

- 9-12.CS.2 Compare levels of abstraction and interactions between application software, system software, and hardware
- 9-12S.CS.2 Categorize and describe the different functions of operating system software

CA Common Core State Standards

- CCSS.ELA-LITERACT.WHST.1: Write arguments focused on discipline-specific content
- CCSS.ELA-LITERACT.WHST.4: Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience

UNIT 4 – NETWORK, INTERNET, AND ETHERNET PROTOCOLS

CA Computer Science Standards

- 9-12.CS.3 Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix errors
- 9-12.NI.5 Describe the design characteristics of the internet
- 9-12S.NI.3 Examine the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing

UNIT 5 – NETWORKING SECURITY, CONNECTIVITY, AND FUNCTIONALITY

CA Computer Science Standards

- 9-12.CS.3 Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix errors
- 9-12.NI.4 Describe issues that impact network functionality
- 9-12.NI.6 Compare and contrast security measures to address various security threats
- 9-12S.NI.3 Examine the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing

CA Common Core State Standards

- CCSS.ELA-LITERACT.WHST.1: Write arguments focused on discipline-specific content
- CCSS.ELA-LITERACT.WHST.2: Write informative/explanatory texts, including the narration of historical events, scientific procedures/ experiments, or technical processes
- CCSS.ELA-LITERACT.WHST.4: Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience
- CCSS.ELA-LITERACY.WHST.5: Develop and strengthen writing as needed by planning, revising, editing, rewriting, or trying a new approach, focusing on addressing what is most significant for a specific purpose and audience
- CCSS.ELA-LITERACY.WHST.6: Use technology, including the Internet, to produce, publish, and update individual or shared writing products in response to ongoing feedback, including new arguments or information
- CCSS.ELA-LITERACY.WHST.8: Gather relevant information from multiple authoritative print and digital sources, using advanced searches effectively; assess the strengths and limitations of each source in terms of the specific task, purpose, and audience; integrate information into the text selectively to maintain the flow of ideas, avoiding plagiarism and overreliance on any one source and following a standard format for citation

UNIT 6 – NETWORK SERVICES, DEVICES, AND SECURITY
CA Computer Science Standards
- 9-12.CS.3 Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix errors
- 9-12.NI.6 Compare and contrast security measures to address various security threats
- 9-12S.NI.3 Examine the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing

UNIT 7 – ATTACKS AND THREATS
CA Computer Science Standards
- 9-12.NI.6 Compare and contrast security measures to address various security threats

UNIT 8 – NETWORK OPERATIONS AND NETWORK ATTACKS
CA Computer Science Standards
- 9-12.CS.3 Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix errors
- 9-12.NI.6 Compare and contrast security measures to address various security threats
- 9-12.NI.4 Describe issues that impact network functionality

UNIT 9 – DEFENSE AND ACCESS
CA Computer Science Standards
- 9-12.NI.6 Compare and contrast security measures to address various security threats
- 9-12S.NI.5 Develop solutions to security threats

UNIT 10 – THREAT INTELLIGENCE AND CRYPTOGRAPHY
CA Computer Science Standards
- 9-12.NI.7 Compare and contrast cryptographic techniques to model the secure transmission of information
- 9-12S.NI.6 Analyze cryptographic techniques to model the secure transmission of information

CA Common Core State Standards
- CCSS.ELA-LITERACT.WHST.1: Write arguments focused on discipline-specific content
- CCSS.ELA-LITERACT.WHST.4: Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience
- CCSS.ELA-LITERACY.WHST.5: Develop and strengthen writing as needed by planning, revising, editing, rewriting, or trying a new approach, focusing on addressing what is most significant for a specific purpose and audience
- CCSS.ELA-LITERACY.WHST.7: Conduct short as well as more sustained research projects to answer a question (including a self- generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation
- CCSS.ELA-LITERACY.WHST.8: Gather relevant information from multiple authoritative print and digital sources, using advanced searches effectively; assess the strengths and limitations of each source in terms of the specific task, purpose, and audience; integrate information into the text selectively to maintain the flow of ideas, avoiding plagiarism and overreliance on any one source and following a standard format for citation
- CCSS.ELA-LITERACY.WHST.9: Draw evidence from informational texts to support analysis, reflection, and research
- CCSS.ELA-LITERACY.WHST.10: Write routinely over extended time frames (time for reflection and revision) and shorter time frames (a single sitting or a day or two) for a range of discipline-specific tasks, purposes, and audiences

UNIT 11 – ENDPOINT PROTECTION AND VULNERABILITY

CA Computer Science Standards

- 9-12S.NI.5 Develop solutions to security threats
- 9-12.NI.6 Compare and contrast security measures to address various security threats

CA Common Core State Standards

- CCSS.ELA-LITERACT.WHST.1: Write arguments focused on discipline-specific content
- CCSS.ELA-LITERACT.WHST.4: Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience
- CCSS.ELA-LITERACY.WHST.5: Develop and strengthen writing as needed by planning, revising, editing, rewriting, or trying a new approach, focusing on addressing what is most significant for a specific purpose and audience
- CCSS.ELA-LITERACY.WHST.7: Conduct short as well as more sustained research projects to answer a question (including a self- generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation
- CCSS.ELA-LITERACY.WHST.8: Gather relevant information from multiple authoritative print and digital sources, using advanced searches effectively; assess the strengths and limitations of each source in terms of the specific task, purpose, and audience; integrate information into the text selectively to maintain the flow of ideas, avoiding plagiarism and overreliance on any one source and following a standard format for citation
- CCSS.ELA-LITERACY.WHST.9: Draw evidence from informational texts to support analysis, reflection, and research
- CCSS.ELA-LITERACY.WHST.10: Write routinely over extended time frames (time for reflection and revision) and shorter time frames (a single sitting or a day or two) for a range of discipline-specific tasks, purposes, and audiences

UNIT 12 – SECURITY TECHNOLOGIES AND PROTOCOLS

CA Computer Science Standards

- 9-12.NI.6 Compare and contrast security measures to address various security threats
- 9-12S.NI.5 Develop solutions to security threats

CA Common Core State Standards

- CCSS.ELA-LITERACT.WHST.1: Write arguments focused on discipline-specific content
- CCSS.ELA-LITERACT.WHST.4: Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience
- CCSS.ELA-LITERACY.WHST.5: Develop and strengthen writing as needed by planning, revising, editing, rewriting, or trying a new approach, focusing on addressing what is most significant for a specific purpose and audience
- CCSS.ELA-LITERACY.WHST.7: Conduct short as well as more sustained research projects to answer a question (including a self- generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation
- CCSS.ELA-LITERACY.WHST.8: Gather relevant information from multiple authoritative print and digital sources, using advanced searches effectively; assess the strengths and limitations of each source in terms of the specific task, purpose, and audience; integrate information into the text selectively to maintain the flow of ideas, avoiding plagiarism and overreliance on any one source and following a standard format for citation
- CCSS.ELA-LITERACY.WHST.9: Draw evidence from informational texts to support analysis, reflection, and research
- CCSS.ELA-LITERACY.WHST.10: Write routinely over extended time frames (time for reflection and revision) and shorter time frames (a single sitting or a day or two) for a range of discipline-specific tasks, purposes, and audiences

UNIT 13 – NETWORK SECURITY: ALERTS, LOGS, AND DATA

CA Computer Science Standards

- 9-12.CS.3 Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix errors
- 9-12S.NI.5 Develop solutions to security threats
- 9-12.NI.4 Describe issues that impact network functionality

UNIT 14 – DIGITAL FORENSICS AND INCIDENT ANALYSIS AND RESPONSE

CA Computer Science Standards

- 9-12.CS.3 Develop guidelines that convey systematic troubleshooting strategies that others can use to identify and fix errors
- 9-12S.NI.5 Develop solutions to security threats

CA Common Core State Standards

- CCSS.ELA-LITERACY.RST.1: Cite specific textual evidence to support analysis of science and technical texts, attending to important distinctions the author makes and to any gaps or inconsistencies in the account
- CCSS.ELA-LITERACY.RST.7: Integrate and evaluate multiple sources of information presented in diverse formats and media (e.g., quantitative data, video, multimedia) in order to address a question or solve a problem
- CCSS.ELA-LITERACY.RST.9: Synthesize information from a range of sources (e.g., texts, experiments, simulations) into a coherent understanding of a process, phenomenon, or concept, resolving conflicting information when possible
- CCSS.ELA-LITERACT.WHST.1: Write arguments focused on discipline-specific content
- CCSS.ELA-LITERACT.WHST.4: Produce clear and coherent writing in which the development, organization, and style are appropriate to task, purpose, and audience
- CCSS.ELA-LITERACY.WHST.5: Develop and strengthen writing as needed by planning, revising, editing, rewriting, or trying a new approach, focusing on addressing what is most significant for a specific purpose and audience
- CCSS.ELA-LITERACY.WHST.6: Use technology, including the Internet, to produce, publish, and update individual or shared writing products in response to ongoing feedback, including new arguments or information
- CCSS.ELA-LITERACY.WHST.7: Conduct short as well as more sustained research projects to answer a question (including a self- generated question) or solve a problem; narrow or broaden the inquiry when appropriate; synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation
- CCSS.ELA-LITERACY.WHST.8: Gather relevant information from multiple authoritative print and digital sources, using advanced searches effectively; assess the strengths and limitations of each source in terms of the specific task, purpose, and audience; integrate information into the text selectively to maintain the flow of ideas, avoiding plagiarism and overreliance on any one source and following a standard format for citation
- CCSS.ELA-LITERACY.WHST.9: Draw evidence from informational texts to support analysis, reflection, and research.
- CCSS.ELA-LITERACY.WHST.10: Write routinely over extended time frames (time for reflection and revision) and shorter time frames (a single sitting or a day or two) for a range of discipline-specific tasks, purposes, and audiences