Course Outline

Information and Communication Technologies **REVISED June/2019**

Course Description:

This competency-based course is designed to prepare the student for the 210-250 SECFND exam. This exam is the first of the two required exams to achieve the CCNA Cyber Ops certification.
This course equips students with the basic knowledge, foundational principles, and entry-level skills needed by today's organizations that are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. The student could be part of a team of people in Security Operations Centers (SOC's) monitoring security systems, protecting their organizations by detecting and responding to cybersecurity threats. Introduction to Cybersecurity Operations prepares candidates to begin a career working with associate-level cybersecurity analysts within Security Operations Centers (SOC's).
In addition, the United States Department of Defense (DoD) has approved Cisco CCNA Cyber Ops Certification for inclusion in the DoD 8570.01-M for the CCSP Analyst and CCSP Incident Responder categories.
The competencies in this course are aligned with the California High School Academic Content Standards and the California Career Technical Education Model Curriculum Standards.

Job Title: Information Security Analyst

Career Pathway: Networking

Industry Sector: Information and Communication Technologies

O*NET-SOC CODE: 15-1122.00

CBEDS Title: Network Security

CBEDS No.: 4646

77-65-70

Cybersecurity Operations Fundamentals

Credits: 10 **Hours:** 120

Prerequisites:
Enrollment requires a 6.0 reading level as measured by the TABE D 9/10, successful completion (or equivalent) of one of the Computer Operation courses (75-35-85, 75-45-50, 75-45-60, 75-45-70), and successful completion (or demonstrate competency) of Algebra I.

This course cannot be repeated once a student receives a Certificate of Completion.

NOTE: For Perkins purposes this course has been designated as an introductory course.

Los Angeles Unified School District
Division of Adult and Career Education
Instructional and Couseling Services Unit
Adult Curriculum Office
www.wearedace.org

COURSE OUTLINE COMPETENCY-BASED COMPONENTS

A course outline reflects the essential intent and content of the course described. Acceptable course outlines have six components. (Education Code Section 52506). Course outlines for all apportionment classes, including those in jails, state hospitals, and convalescent hospitals, contain the six required elements:

(EC 52504; 5CCR 10508 [b]; Adult Education Handbook for California [1977], Section 100)

COURSE OUTLINE COMPONENTS	**LOCATION**
GOALS AND PURPOSES	Cover
The educational goals or purposes of every course are clearly stated and the class periods are devoted to instruction. The course should be broad enough in scope and should have sufficient educational worth to justify the expenditure of public funds.	
The goals and purpose of a course are stated in the COURSE DESCRIPTION. Course descriptions state the major emphasis and content of a course, and are written to be understandable by a prospective student.	
PERFORMANCE OBJECTIVES OR COMPETENCIES	pp. 7-13
Objectives should be delineated and described in terms of measurable results for the student and include the possible ways in which the objectives contribute to the student's acquisition of skills and competencies.	
Performance Objectives are sequentially listed in the COMPETENCY-BASED COMPONENTS section of the course outline. Competency Areas are units of instruction based on related competencies. Competency Statements are competency area goals that together define the framework and purpose of a course. Competencies fall on a continuum between goals and performance objectives and denote the outcome of instruction.	
Competency-based instruction tells a student before instruction what skills or knowledge they will demonstrate after instruction. Competency-based education provides instruction which enables each student to attain individual goals as measured against pre-stated standards.	
Competency-based instruction provides immediate and continual repetition and in competency-based education the curriculum, instruction, and assessment share common characteristics based on clearly stated competencies. Curriculum, instruction and assessment in competency-based education are: explicit, known, agreed upon, integrated, performance oriented, and adaptive.	

COURSE OUTLINE COMPETENCY-BASED COMPONENTS (continued)

COURSE OUTLINE COMPONENTS	LOCATION
INSTRUCTIONAL STRATEGIES	p. 15
Instructional techniques or methods could include laboratory techniques, lecture method, small-group discussion, grouping plans, and other strategies used in the classroom. Instructional strategies for this course are listed in the TEACHING STRATEGIES AND EVALUATION section of the course outline. Instructional strategies and activities for a course should be selected so that the overall teaching approach takes into account the instructional standards of a particular program, i.e., English as a Second Language, Programs for Adults with Disabilities.	
UNITS OF STUDY, WITH APPROXIMATE HOURS ALLOTTED FOR EACH UNIT	Cover
The approximate time devoted to each instructional unit within the course, as well as the total hours for the course, is indicated. The time in class is consistent with the needs of the student, and the length of the class should be that it ensures the student will learn at an optimum level. Units of study, with approximate hours allotted for each unit are listed in the COMPETENCY AREA STATEMENT(S) of the course outline. The total hours of the course, including work-based learning hours (community classroom and cooperative vocational education) is listed on the cover of every CBE course outline. Each Competency Area listed within a CBE outline is assigned hours of instruction per unit.	pp. 7-13
EVALUATION PROCEDURES	p. 15
The evaluation describes measurable evaluation criteria clearly within the reach of the student. The evaluation indicates anticipated improvement in performances as well as anticipated skills and competencies to be achieved. Evaluation procedures are detailed in the TEACHING STRATEGIES AND EVALUATION section of the course outline. Instructors monitor students' progress on a continuing basis, assessing students on attainment of objectives identified in the course outline through a variety of formal and informal tests (applied performance procedures, observations, and simulations), paper and pencil exams, and standardized tests.	
REPETITION POLICY THAT PREVENTS PERPETUATION OF STUDENT ENROLLMENT	Cover
After a student has completed all the objectives of the course, he or she should not be allowed to reenroll in the course. There is, therefore, a need for a statement about the conditions for possible repetition of a course to prevent perpetuation of students in a particular program for an indefinite period of time.	

ACKNOWLEDGMENTS

Thanks to ROBERT YORGASON and ALEJANDRA SALCEDO for developing and editing this course outline. Acknowledgment is also given to ERICA ROSARIO for designing the original artwork for the course covers.

ANA MARTINEZ
Specialist
Career Technical Education

ROSARIO GALVAN
Administrator
Division of Adult and Career Education

APPROVED:

JOSEPH STARK
Executive Director
Division of Adult and Career Education

1.0 Academics
Analyze and apply appropriate academic standards required for successful industry sector pathway completion leading to postsecondary education and employment. Refer to the Agriculture and Natural Resources academic alignment matrix for identification of standards

2.0 Communications
Acquire and accurately use Agriculture and Natural Resources sector terminology and protocols at the career and college readiness level for communicating effectively in oral, written, and multimedia formats.

3.0 Career Planning and Management
Integrate multiple sources of career information from diverse formats to make informed career decisions, solve problems, and manage personal career plans

4.0 Technology
Use existing and emerging technology to investigate, research, and produce products and services, including new information, as required in the Agriculture and Natural Resources sector workplace environment.

5.0 Problem Solving and Critical Thinking
Conduct short as well as more sustained research to create alternative solutions to answer a question or solve a problem unique to the Agriculture and Natural Resources sector, using critical and creative thinking, logical reasoning, analysis, inquiry, and problem-solving techniques.

6.0 Health and Safety
Demonstrate health and safety procedures, regulations, and personal health practices and determine the meaning of symbols, key terms, and domain-specific words and phrases as related to the Agriculture and Natural Resources sector workplace environment.

7.0 Responsibility and Flexibility
Initiate, and participate in, a range of collaborations demonstrating behaviors that reflect personal and professional responsibility, flexibility, and respect in the Agriculture and Natural Resources sector workplace environment and community settings.

8.0 Ethics and Legal Responsibilities
Practice professional, ethical, and legal behavior, responding thoughtfully to diverse perspectives and resolving contradictions when possible, consistent with applicable laws, regulations, and organizational norms.

9.0 Leadership and Teamwork
Work with peers to promote divergent and creative perspectives, effective leadership, group dynamics, team and individual decision making, benefits of workforce diversity, and conflict resolution as practiced in the Future Farmers of America (FFA) career technical student organization.

10.0 Technical Knowledge and Skills
Apply essential technical knowledge and skills common to all pathways in the Agriculture and Natural Resources sector, following procedures when carrying out experiments or performing technical tasks.

11.0 Demonstration and Application
Demonstrate and apply the knowledge and skills contained in the Agriculture and Natural Resources anchor standards, pathway standards, and performance indicators in classroom, laboratory, and workplace settings, and through the FFA career technical student organization.

B. Networking Pathway

Students in the Networking pathway prepare for careers that involve the implementation of computer services and software, support of multimedia products and services, provision of technical assistance, creation of technical documentation, and the administration and management of information and communication systems. Mastery of information and communication technologies is the foundation for all successful business organizations today. Persons with expertise in information and communication technologies support and services are in high demand for a variety of positions in business and industry.

Sample occupations associated with this pathway:

- Information Security Analyst
- Computer and Information Systems Manager
- Computer User Support Specialist
- Database Administrator
- Document Management Specialist
- Business Intelligence Analyst

B1.0 Identify, and describe the principles of networking and the technologies, models, and protocols used in a network.

B2.0 Identify, describe, and implement network media and physical topologies.

B3.0 Install, configure, and differentiate between common network devices.

B4.0 Demonstrate proper network administration and management skills.

B5.0 Demonstrate how to communicate and interpret information clearly in industry-standard visual and written formats.

B6.0 Use and assess network communication applications and infrastructure.

B7.0 Analyze a customer's organizational needs and requirements to identify networking needs.

B8.0 Identify security threats to a network and describe general methods to mitigate those threats.

COMPETENCY-BASED COMPONENTS
for the Cybersecurity Operations Fundamentals Course

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
A. ORIENTATION AND SAFETY Understand, apply, and evaluate classroom and workplace policies and procedures used in accordance with federal, state, and local safety and environmental regulations. (4 hours)	1. Describe the scope and purpose of the course. 2. Describe the overall course content as a part of the linked Learning Initiative. 3. Describe classroom policies and procedures. 4. Identify classroom and workplace first aid and emergency procedures based on the American Red Cross (ARC) standards. 5. Describe the different occupations in the Information and Communication Technologies industry sector, which have an impact on the role of computer technicians. 6. Describe the opportunities available for promoting gender equity and the representation of non-traditional populations in computer technology. 7. Explain the impact of Environmental Protection Agency (EPA) legislation on the Information and Communication Technologies industry sector practices in protecting and preserving the environment. 8. Describe and demonstrate the procedures for contacting proper authorities for the removal of hazardous materials based on the EPA standards. 9. Describe and demonstrate the use of the Material Safety Sheet (MSDS) as it applies to the Information and Communication Technologies industry sector. 10. Describe the California Occupational Safety and Health Administration (Cal/OSHA) and its laws governing information security analysts. 11. Describe how each of the following insures a safe workplace: a) Employees' rights as they apply to job safety b) Employees' obligations as they apply to safety c) Safety laws applying to electrical tools d) Proper use of static straps and static mats 12. Pass the safety exam with 100% accuracy.	**Career Ready Practice:** 1, 2, 4, 7, 8, 12 **CTE Anchor:** Communications: 2.3, 2.4, 2.5 Technology: 4.5, 4.6 Health and Safety: 6.2, 6.3 Ethics and Legal Responsibilities: 8.2, 8.5 Technical Knowledge and Skills: 10.1, 10.2, 10.4 Demonstration and Application: 11.2 **CTE Pathway:** B1.1
B. NETWORK CONCEPTS Identify and describe the principles of networking and the technologies, models,	1. Describe the function of the network layers as specified by the OSI and the TCP/IP network models 2. Describe the operation of the following protocols. a) Internet Protocol (IP) b) Transport Protocol (TCP)	**Career Ready Practice:** 1, 2, 8, 12 **CTE Anchor:** Communications:

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
services, and protocols used in a network. Explain the operation of the network infrastructure. (20 hours)	c) User Datagram Protocol (UDP) d) Internet Control Message Protocol (ICMP) 3. Describe the operation of these network services a) Address Resolution Protocol (ARP) b) Domain Name Service (DNS) c) Dynamic Host Configuration Protocol (DHCP) 4. Describe the basic operation of these network devices a) Router b) Switch c) Hub d) Bridge e) Wireless access point (WAP) f) Wireless LAN controller (WLC) 5. Describe the functions of these network security systems as deployed on the host, network, or the cloud: a) Firewall b) Intrusion Prevention System (IPS) c) Advanced Malware Protection (AMP) d) Web Security Appliance (WSA) e) Cloud Web Security (CWS) f) Email Security Appliance (ESA) g) Cloud Email Security (CES) 6. Describe IP subnets and communication within an IP subnet and between IP subnets 7. Describe the relationship between Virtual Local Area Networks (VLANs) and data visibility 8. Describe the operation of Access Control Lists (ACLs) applied as packet filters on the interfaces of network devices 9. Describe Deep Packet Inspection (DPI) 10. Describe packet filtering 11. Describe stateful firewalls 12. Compare and contrast DPI with packet filtering and stateful firewall operation 13. Describe a network tap 14. Describe network traffic mirroring 15. Describe net flow 16. Compare and contrast inline traffic inspection and taps or traffic mirroring 17. Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic 18. Identify potential data loss from provided traffic profiles	2.5, 2.6 Technology: 4.1, 4.2, 4.4, 4.5 Problem Solving and Critical Thinking: 5.3, 5.4, 5.5, 5.6, 5.11, 5.12 Ethics and Legal Responsibilities: 8.3, 8.6, 8.8 Technical Knowledge and Skills: 10.1, 10.5, 10.11 **CTE Pathway:** B1.1, B1.2, B1.3, B1.5, B1.6, B2.1, B3.1, B3.3, B5.1, B8.4
C. COMPUTER MATH Apply and evaluate the powers of two, ten, sixteen, metric	1. Identify the practical applications of math in networks. 2. Describe the metric prefixes (engineering prefixes) 3. Describe the number systems associated with computers and computer networks	**Career Ready Practice:** 1, 2, 4, 5

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
prefixes. Apply and use the binary, decimal, and hexadecimal number systems. (17 hours)	4. Describe the powers of ten and decimal number system. 5. Describe the binary number system and the powers of two. 6. Describe the hexadecimal number system. 7. Describe and demonstrate the conversion of binary numbers to decimal numbers. 8. Describe and demonstrate the conversion of decimal numbers to hexadecimal numbers. 9. Describe and demonstrate the conversion of hexadecimal numbers to binary numbers. 10. Calculate and identify IPv4 network, subnetwork, and host addresses.	**CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3 Problem Solving and Critical Thinking 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 Technical Knowledge and Skills: 10.6, 10.7 **CTE Pathway:** B1.1, B1.6, B5.2
D. SECUIRTY CONCEPTS Classify the various types of network attacks. Explain how networks are attacked. Explain the various types of threats and attacks. Use various methods to prevent malicious access to computer networks, hosts, and data	1. Describe the principles of the defense in depth strategy 2. Compare and contrast these concepts a) Risk b) Threat c) Vulnerability d) Exploit 3. Describe these terms a) Threat actor b) Run book automation (RBA) c) Chain of custody (evidentiary) d) Reverse engineering e) Sliding window anomaly detection f) Personally Identifiable Information (PII) g) Protected Health Information (PHI) 4. Describe these security terms a) Principle of least privilege b) Risk scoring/risk weighting c) Risk reduction d) Risk assessment 5. Compare and contrast these access control models a) Discretionary access control b) Mandatory access control c) Non-discretionary access control 6. Compare and contrast these terms a) Network and host antivirus b) Agentless and agent-based protections c) SIEM and log collection 7. Describe these concepts a) Asset management b) Configuration management	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3 Problem Solving and Critical Thinking: 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10 Technical Knowledge and Skills: 10.6, 10.7 **CTE Pathway:** B1.1, B1.2, B1.5, B1.6, B5.1, B8.1, B8.4

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(16 hours)	c) Mobile device management d) Patch management e) Vulnerability management	
E. CRYPTOGRAPHY Explain the impacts of cryptography on network security. Explain how the public key infrastructure (PKI) supports network security. Use tools to encrypt and decrypt data (6 hours)	1. Describe the uses of a hash algorithm 2. Describe the uses of encryption algorithms 3. Compare and contrast symmetric and asymmetric encryption algorithms 4. Describe the processes of digital signature creation and verification 5. Describe the operation of a Public Key Infrastructure (PKI) 6. Describe the security impact of these commonly used hash algorithms a) Message Digest 5 (MD5) b) Secure Hash Algorithm 1 (SHA-1) c) Secure Hash Algorithm 256 (SHA-256) d) Secure Hash Algorithm 512 (SHA-512) 7. Describe the security impact of these commonly used encryption algorithms and secure communications protocols a) Data Encryption Standard (DES) b) 3DES c) Advanced Encryption Standard (AES) d) AES256-CTR e) RSA f) Digital Signature Algorithm (DSA) g) Secure Shell Handler (SSH) h) SSL/TLS 8. Describe how the success or failure of a cryptographic exchange impacts security investigation 9. Describe these items in regards to Secure Sockets Layer (SSL) and Transport Layer Security (TLS) a) Cipher-suite b) X.509 certificates c) Key exchange d) Protocol version e) PKCS	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3 Problem Solving and Critical Thinking: 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 Technical Knowledge and Skills: 10.8 **CTE Pathway:** B1.1, B1.2, B1.5, B1.6, B5.1, B8.4
F. HOST BASED ANALYSIS Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses. Explain the features and characteristics of the Linux Operating System. Perform	1. Define these terms as they pertain to Microsoft Windows a) Processes b) Threads c) Memory allocation d) Windows Registry e) Windows Management Instrumentation (WMI) f) Handles g) Services 2. Define these terms as they pertain to Linux a) Processes	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
basic tasks to secure Windows and Linux operating systems. (17 hours)	b) Forks c) Permissions d) Symlinks e) Daemon 3. Describe the functionality of these endpoint technologies in regards to security monitoring a) Host-based intrusion detection b) Antimalware and antivirus c) Host-based firewall d) Application-level whitelisting/blacklisting e) Systems-based sandboxing (such as Chrome, Java, Adobe reader) 4. Interpret these operating system log data to identify an event a) Windows security event logs b) Unix-based syslog c) Apache access logs d) IIS access logs	Problem Solving and Critical Thinking: 5.1, 5.2, 5.3, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 Technical Knowledge and Skills: 10.1, 10.8, 10.10 **CTE Pathway:** B1.1, B1.6, B4.1, B5.1, B8.4
G. SECURITY MONITORING Evaluate network security alerts, explain the differing types of security technologies and how they impact security monitoring, explain the types of log files used in security monitoring. Use network monitoring tools to identify attacks that against network protocols and services	1. Identify the types of data provided by these technologies a) TCP Dump b) NetFlow c) Next-Gen firewall d) Traditional stateful firewall e) Application visibility and control f) Web content filtering g) Email content filtering 2. Describe these types of data used in security monitoring a) Full packet capture b) Session data c) Transaction data d) Statistical data e) Extracted content f) Alert data 3. Describe these network concepts as they relate to security monitoring a) Access Control List (ACL) b) Network Address Translation (NAT), Port Address Translation (PAT) c) Tunneling d) The Onion Router (TOR) e) Encryption f) P2P g) Encapsulation h) Load balancing 4. Describe these NextGen IPS event types a) Connection event b) Intrusion event c) Host or endpoint event	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3 Problem Solving and Critical Thinking: 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 Technical Knowledge and Skills: 10.6, 10.7 **CTE Pathway:** B1.1, B1.2, B1.5, B1.6, B4.1,B4.3, B5.1, B8.2, B8.4

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
(17 hours)	d) Network discovery event e) NetFlow event 5. Describe the function of these protocols in the context of security monitoring a) DNS b) NTP c) SMTP/POP/IMAP d) HTTP/HTTPS	
H. ATTACK METHODS Explain how to investigate endpoint vulnerabilities and classify endpoint vulnerability assessment information. (18 hours)	1. Compare and contrast an attack surface and vulnerability 2. Describe these network attacks a) Denial of service (DoS) b) Distributed denial of service (DDoS) c) Man-in-the-middle (MitM) 3. Describe these web application attacks a) Structured Query Language (SQL) injection b) Command injections c) Cross-site scripting 4. Describe these attacks a) Social engineering b) Phishing c) Evasion methods 5. Describe these endpoint-based attacks a) Buffer overflows b) Command and control (C2) c) Malware d) Rootkit e) Port scanning f) Host profiling 6. Describe these evasion methods a) Encryption and tunneling b) Resource exhaustion c) Traffic fragmentation d) Protocol-level misinterpretation e) Traffic substitution and insertion f) Pivot g) Define privilege escalation 7. Compare and contrast remote exploit and a local exploit	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Communications: 2.5 Technology: 4.2, 4.3 Problem Solving and Critical Thinking: 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10 Technical Knowledge and Skills: 10.6, 10.7 **CTE Pathway:** B1.1, B1.2, B1.5, B1.6, B5.1, B8.1, B8.4
I. EMPLOYABILITY SKILLS Understand, apply, and evaluate the employability skills required in the Cybersecurity field. Understand the requirements	1. Identify steps required to obtain the CCNA Cyber Ops certification: a) Identify the first exam (210-250) required for CCNA Cyber Ops certification b) Identify the second exam required (210-255) required for CCN Cyber Ops certification. c) Explain the registration process for certification exams. d) Describe the exam testing environment. 2. Identify other Cybersecurity certifications	**Career Ready Practice:** 1, 2, 3, 4, 6, 7, 8, 9, 11, 12 **CTE Anchor:** Communications:

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
and procedures for obtaining a CCNA CyberOps certification. (5 hours)	a) Describe DoD Directive 8570 baseline certifications b) Describe the International Information Systems Security Certification Consortium (ISC2). c) Identify job titles and required industry certifications 3. Summarize employers requirements for the following: a) Identify potential employers through traditional and internet b) sources. c) Describe the role of social media in job search. d) Design sample résumés and covers letters. e) Explain the importance of filling out a job application legibly, with accurate and complete information. f) Describe the common mistakes that are made on job applications. g) Complete sample job application forms correctly. h) State the importance of enthusiasm in the interview and on a job. i) State the importance of appropriate appearance in the interview and on a job. j) State the importance of the continuous upgrading of job skills. k) Describe customer service as a method of building permanent relationships between the organization and the customer. l) Describe and Demonstrate appropriate interviewing techniques. m) Identify the informational materials and resources needed to be successful in an interview. n) Design sample follow-up letters. o) Describe and demonstrate appropriate follow-up procedures.	2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8 Career Planning Management: 3.1, 3.2, 3.3, 3.4, 3.8 Technology: 4.5 Demonstration and Application: 11.2, 11.5 **CTE Pathway:** B7.1, B7.3

SUGGESTED INSTRUCTIONAL MATERIALS and OTHER RESOURCES

TEXTS AND SUPPLEMENTAL BOOKS

Omar Santos, Joseph Muniz, Stefano De Crescenzo CCNA Cyber Ops SECFND #210-250 Official Cert Guide. Cisco Press 2017 ISBN-10: 1-58714-702-5

Cisco Press (Author) - CCNA Cybersecurity Operations Companion Guide 1st Edition, Cisco Press 2018 ISBN-10: 158713439X

ITSpecialist (Author) - CCNA Cyber Ops (SECFND 210 - 250) Complete Training Guide with Practice Exam Questions ITSpecialist 2018 ISBN-10: 172924436X

ONLINE SOFTWARE

Cisco Networking Academy http://netacad.com

SOFTWARE

Oracle VirtualBox (Free) https://www.virtualbox.org/

Virtual Machines (Free)

- Security Onion https://securityonion.net/
- Kali Linux https://www.kali.org/
- Metasploitable https://metasploit.help.rapid7.com/docs/
- CyberOps Skills Challenge Client and Server available from Cisco Networking Academy

RESOURCES

Employer Advisory Board Meetings

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity
https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

CTE Foundation Standards
http://www.cde.ca.gov/ci/ct/sf/documents/ctestandards.pdf
http://www.cde.ca.goc/be/st/ss/documents/ctestandards.doc

TEACHING STRATEGIES and EVALUATION

METHODS AND PROCEDURES

A. Lecture and discussion

B. Multimedia presentations

C. Demonstrations and Hands-on Labs

D. Individualized instruction

E. Peer teaching

F. Role-playing

G. Guest speakers

H. Field trips and field study experiences

I. Projects

EVALUATION

SECTION A – Orientation and Safety – Pass the safety test with 100% accuracy.

SECTION B– Network Concepts - Pass all assignments and exams on network concepts with a minimum score of 80% or higher.

SECTION C – Computer Math – Pass all assignments and exams on computer math with a minimum score of 80% or higher.

SECTION D – Security Concepts – Pass all assignments and exams on security concepts with a minimum score of 80% or higher.

SECTION E – Cryptography – Pass all assignments and exams on cryptography with a minimum score of 80% or higher.

SECTION F – Host Based Analysis – Pass all assignments and exams on host based analysis with a minimum score of 80% or higher.

SECTION G – Security Monitoring – Pass all assignments and exams on security monitoring with a minimum score of 80% or higher.

SECTION H – Attack methods – Pass all assignments and exams on attack methods with a minimum score of 80% or higher.

SECTION I – Employability Skills – Pass all assignments and exams on employability skills with a minimum score of 80% or higher.

Statement for Civil Rights

All educational and vocational opportunities are offered without regard to race, color, national origin, gender, or physical disability.