CNIT R145: COMPTIA SECURITY+ IT SECURITY AND CERTIFICATION PREPARATION

Originator
alynch

College
Oxnard College

Discipline (CB01A)
CNIT - Computer Networking/IT

Course Number (CB01B)
R145

Course Title (CB02)
CompTIA Security+ IT Security and Certification Preparation

Banner/Short Title
CompTIA Security+ IT Security

Credit Type
Credit

Start Term
Fall 2020

Formerly
ENGT R145

Catalog Course Description
The CompTIA Security+ course covers a wide variety of IT security topics at a foundation level including host security, network security, security issues related to cloud computing, vulnerabilities and threats, risk assessment and risk mitigation, and security policies. The course also covers access control, identity management, incident management, wireless network security, and cryptography. This course includes hands on cybersecurity training labs. Students who successfully complete this course should be prepared for the CompTIA Security+ certification exam which is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.

Taxonomy of Programs (TOP) Code (CB03)
0708.10 - *Computer Networking

Course Credit Status (CB04)
D (Credit - Degree Applicable)

Course Transfer Status (CB05) (select one only)
B (Transferable to CSU only)

Course Basic Skills Status (CB08)
N - The Course is Not a Basic Skills Course

SAM Priority Code (CB09)
C - Clearly Occupational

Course Cooperative Work Experience Education Status (CB10)
N - Is Not Part of a Cooperative Work Experience Education Program

Course Classification Status (CB11)
Y - Credit Course

Educational Assistance Class Instruction (Approved Special Class) (CB13)
N - The Course is Not an Approved Special Class

Course Prior to Transfer Level (CB21)
Y - Not Applicable

Course Noncredit Category (CB22)
Y - Credit Course

Funding Agency Category (CB23)
Y - Not Applicable (Funding Not Used)

Course Program Status (CB24)
1 - Program Applicable

General Education Status (CB25)
Y - Not Applicable

Support Course Status (CB26)
N - Course is not a support course

Field trips
May be required

Grading method
Letter Graded

Alternate grading methods
Credit by exam, license, etc.

Does this course require an instructional materials fee?
No

Repeatable for Credit
No

Units and Hours

Carnegie Unit Override
No

In-Class

Lecture
Minimum Contact/In-Class Lecture Hours
43.75

Activity

Laboratory
Minimum Contact/In-Class Laboratory Hours
26.25

Total in-Class

Total in-Class
Total Minimum Contact/In-Class Hours
70

Outside-of-Class

Internship/Cooperative Work Experience

Paid

Unpaid

Total Outside-of-Class

Total Outside-of-Class
Minimum Outside-of-Class Hours
87.5

Total Student Learning

Total Student Learning
Total Minimum Student Learning Hours
157.5

Minimum Units (CB07)
3
Maximum Units (CB06)
3

Advisories on Recommended Preparation
CNIT R101 or CNIT R120 or CNIT R142 or CNIT R144

Student Learning Outcomes (CSLOs)

	Upon satisfactory completion of the course, students will be able to:
1	Students will conduct research using computer networking security websites to identify the most recent threats to networks and the steps that should be taken to mitigate those threats.
2	Students will be able to configure a firewall on an Integrated Service Router (ISR) to deny access to the network based on source IP address and port number.
3	Create a security policy for a fictitious organization and implement elements of the security policy using technology such as the password policy.
4	Configue a wireless router and clients with enterprise class WLAN security.

Course Objectives

	Upon satisfactory completion of the course, students will be able to:
1	Differentiate and explain access control models
2	Compare and contrast various authentication methods
3	Identify non-essential protocols that pose a security risk
4	Recognize attack methods and actions to take to mitigate risk
5	Identify malicious code and appropriate actions to reduce vulnerability
6	Understand the concept of social engineering and the risk it poses
7	Log and record data
8	Identify and define various remote access technologies
9	Understand the administration of email security concepts
10	Compare and contrast Internet security concepts
11	Differentiate and explain wireless security protocols
12	Evaluate security concerns on hardware devices
13	Identify security concerns of different networking media
14	Analyze types of intrusion detection systems
15	Compare cryptography algorithms and summarize strength of each type of algorithm

16 List the steps that are necessary to deal with a cybersecurity incident

17 Differentiate between the different cloud coputing models

Course Content

Lecture/Course Content

1. Access Control Models
   1. Mandatory Access Control (MAC)
   2. Discretionary Access Control (DAC)
   3. Role Based Access Control (RBAC)
2. Authentication Methods
   1. Kerberos
   2. Biometrics
   3. Certificates
3. Protocols and Vulnerabilities
   1. Essential protocols including TCP/IP, DHCP, DNS, SNMP and their vulnerabilities
   2. Non-essential protocols that can be disabled
4. Attack Methods
   1. Spoofing
   2. TCP/IP Hijacking
   3. Replay attacks
5. Malicious Code
   1. Viruses
   2. Trojan Horses
   3. Worms
6. Social Engineering
   1. Role playing
   2. Email, phone, and personnel vulnerabilities
   3. Reducing risk of social engineering
7. Maintaining Data Records
   1. Auditing
   2. Logging
   3. Scanning tools
8. Remote Access Technologies
   1. 802.1x
   2. VPN, RADIUS, PPTP
   3. SSH, IP Sec
9. Email Security
   1. Multipurpose Internet Mail Extensions (MIME)
   2. Pretty Good Privacy (PGP)
   3. SPAM
10. Internet Security
    1. Secure Sockets Layer / Transport Layer Security
    2. Instant messaging vulnerabilities
    3. Active X, cookies, signed applets
11. Wireless Security Protocols
    1. 802.11 and 802.1x
    2. WEP/WPA/WPAII and Enterprise Mode
    3. Site Surveys
12. Security Concerns on Hardware Devices
    1. Firewalls
    2. Routers, switches, hubs
    3. Workstations and servers
13. Security Concerns of Networking Media
    1. Unshielded twisted pair and shielded twisted pair
    2. Fiber optic cable
    3. Removable media
14. Intrusion Detection Systems
    1. Active detection
    2. Passive detection
    3. Packet analyzers
15. Cryptography Algorithms
    1. Hashing

    2. Symmetric and asymmetric
    3. Key usage

16. Cloud Computing
17. Incident Management

Laboratory or Activity Content

1. Switch
    a. Encrypt all login lines
    b. Port Security
    c. VLANs
    d. DHCP Snooping
2. Router
    a. Encrypt all login lines
    b. Authentication for routing protocols
    c. Subnetting and VLSM
    d. Routing betweeen VLANs
3. Protocol Analyzer
    a. Examine protocol traffic
    b. Capture and analyze unencrypted network traffic (HTTP, Telnet, DNS)
    c. Capture and analyze encrypted network traffic (SSH, TLS, IPSec, HTTPS)
    d. Analyze network addresses
    e. Baseline network usage measurements
4. Firewall
    a. Host-based firewall
    b. Network-based firewall
    c. Stateless packet inspection firewall (ACL)
    d. Statefull packet inspection firewall
5. Intrusion Detection/Prevention System (IDS/IPS)
    a. Host-based IDS
    b. Network-based IDS
    c. Host-based IPS
    d. Network-based IPS
6. Anti-Malware Software Suite
    a. Worm
    b. Virus
    c. Trojan horse
    d. Spam
    e. Phishing
    f. Ransomware
    g. Botnet
    h. Active scanning
7. Virtual Private Network (VPN)
    a. Client configuration
    b. Server configuration
    c. Embedded OS solutions
    d. Encryption options
8. Encryption
    a. EFS file/folder encryption
    b. BitLocker drive encryption
    c. BitLocker to Go USB encryption
    d. IPv6 IPSec encryption
    e. HTTPS web browswer encryption
    f. Digital certificates
    g. Certificate authority
    h. Certificate revocation
9. WLAN Security

Methods of Evaluation

Which of these methods will students use to demonstrate proficiency in the subject matter of this course? (Check all that apply):

Problem solving exercises
Skills demonstrations
Written expression

Methods of Evaluation may include, but are not limited to, the following typical classroom assessment techniques/required assignments (check as many as are deemed appropriate):

Computational homework
Essays
Group projects
Individual projects
Laboratory reports
Objective exams
Oral presentations
Projects
Problem-Solving Assignments
Problem-solving exams
Quizzes
Reports/papers
Skills demonstrations
Skill tests

Instructional Methodology

Specify the methods of instruction that may be employed in this course

Computer-aided presentations
Collaborative group work
Class activities
Class discussions
Case studies
Distance Education
Demonstrations
Field trips
Group discussions
Guest speakers
Instructor-guided use of technology
Internet research
Laboratory activities
Lecture
Small group activities

Describe specific examples of the methods the instructor will use:

1. Instructor will use PowerPoints provided by the publisher to lecture on chapter cybersecurity topics.
2. The instructor will provide a demonstration on how to properly configure a firewall prior to the students beginning their lab.
3. The instructor will summarize cybersecurity current events and ask students critical thinking questions.
4. The instructor will form small groups and have each group research a specific cybersecurity company. The group will create a short presentation to share their research with the class to include company background, target market, and product offerings.

Representative Course Assignments

Writing Assignments

1. Lab entries responding to questions and comparing and contrasting topics such as authentication methods and cryptography.
2. Summarization of a current event topic such as new ransomware, hacking tools and techniques, and massive security breaches.
3. Written and sometimes oral summaries of cybersecurity current events.

Critical Thinking Assignments

1. Evaluation of a cybersecurity vulnerability and specific written recommendations to mitigate the risk.
2. Investigation of a cybersecurity incident and a methodical approach to deal with the incident that is commensurate with industry best practices.

Reading Assignments

1. Reading assignments from Security+ course curriculum.
2. Online sources such as http://www.comptia.org, www.sans.org (http://www.sans.org), and https://www.us-cert.gov/ncas/tips.
3. Cybersecurity vendor websites to learn about their business and line of cybersecurity products.
4. Customizing a security policy to meet the needs of a fictitious company.

Skills Demonstrations

1. Students will demonstrate the ability to configure host based security by hardening the device as specified in a lab assignment.

2. Students will demonstrate the ability to configure a firewall with the appropriate security settings that are specified in a lab assignment.

Other assignments (if applicable)

1. CompTIA Security+ certification prep questions and simulated Security+ certification exams.

Outside Assignments

Representative Outside Assignments

1. Reading the Security+ curriculum.
2. Completing embedded security virtual lab activities.
3. Performing Security+ cert prep review including performance based questions.
4. Reading assigned cybersecurity current event articles to stay abreast of current issues in the field that relate to what is being covered in the curriculum.

Articulation

C-ID Descriptor Number

ITIS 160

Status

Aligned

Equivalent Courses at 4 year institutions

University	Course ID	Course Title	Units
Western Governor's University	C 172	Network and Security - Foundations	3

Comparable Courses within the VCCCD

CNSE M82 - Introduction to Network Security

Equivalent Courses at other CCCs

College	Course ID	Course Title	Units
SBCC	CNEE 120	Introduction to Cybersecurity	4

District General Education

A. Natural Sciences

B. Social and Behavioral Sciences

C. Humanities

D. Language and Rationality

E. Health and Physical Education/Kinesiology

F. Ethnic Studies/Gender Studies

Course is CSU transferable

Yes

CSU Baccalaureate List effective term:
Fall 2013 (was on CSU GE list as ENGT R145 beginning Fall 2006)

CSU GE-Breadth

Area A: English Language Communication and Critical Thinking

Area B: Scientific Inquiry and Quantitative Reasoning

Area C: Arts and Humanities

Area D: Social Sciences

Area E: Lifelong Learning and Self-Development

CSU Graduation Requirement in U.S. History, Constitution and American Ideals:

IGETC

Area 1: English Communication

Area 2A: Mathematical Concepts & Quantitative Reasoning

Area 3: Arts and Humanities

Area 4: Social and Behavioral Sciences

Area 5: Physical and Biological Sciences

Area 6: Languages Other than English (LOTE)

Textbooks and Lab Manuals

Resource Type
Textbook

Description
TestOut Network Security Pro, Security+ SY0-501, CompTIA Approved Quality Content, ISBN: 978-1-935080-44-2, Published 2018

Resource Type
Other Instructional Materials

Description
Hardware devices including hubs, switches, routers, access points, end devices, and firewalls.

Resource Type
Other Instructional Materials

Description
Software such as a operating systems, port scanner, virus scanner, configuration utility, packet analyzer. & vulnerability assessment and pen testing software.

Distance Education Addendum

Definitions

Distance Education Modalities

Hybrid (51%–99% online)
Hybrid (1%–50% online)
100% online

Faculty Certifications

Faculty assigned to teach Hybrid or Fully Online sections of this course will receive training in how to satisfy the Federal and state regulations governing regular effective/substantive contact for distance education. The training will include common elements in the district-supported learning management system (LMS), online teaching methods, regular effective/substantive contact, and best practices.

Yes

Faculty assigned to teach Hybrid or Fully Online sections of this course will meet with the EAC Alternate Media Specialist to ensure that the course content meets the required Federal and state accessibility standards for access by students with disabilities. Common areas for discussion include accessibility of PDF files, images, captioning of videos, Power Point presentations, math and scientific notation, and ensuring the use of style mark-up in Word documents.

Yes

Regular Effective/Substantive Contact

Hybrid (1%–50% online) Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity for the instructor and students to provide feedback.
Face to Face (by student request; cannot be required)	Part of the course requires face to face time. Also, face to face with individuals will take place to discuss specific questions, issues or concerns.
E-mail	Email will be used for individual interaction between professor and student, to send group reminders of deadlines, and to inform of upcoming course content.
Video Conferencing	Video conferencing software may be utilized so the instructor can have synchronous visual and audible communication with students.

Hybrid (51%–99% online) Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity for the instructor and students to provide feedback.
E-mail	Email will be used for individual interaction between professor and student, to send group reminders of deadlines, and to inform of upcoming course content.
Face to Face (by student request; cannot be required)	Part of the course requires face to face time. Also, face to face with individuals will take place to discuss specific questions, issues or concerns.
Video Conferencing	Video conferencing software may be utilized so the instructor can have synchronous visual and audible communication with students.

100% online Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity for the instructor and students to provide feedback.

E-mail	Email will be used for individual interaction between professor and student, to send group reminders of deadlines, and to inform of upcoming course content.
Video Conferencing	Video conferencing software may be utilized so the instructor can have synchronous visual and audible communication with students.
Synchronous Dialog (e.g., online chat)	Online chat will provide the opportunity for discussions and to answer questions and provide feedback on course progress and feedback on assignments and virtual lab assignments.

Examinations

Hybrid (1%–50% online) Modality

Online
On campus

Hybrid (51%–99% online) Modality

On campus

Primary Minimum Qualification

COMPUTER INFORMATION SYS

Additional local certifications required

Current CompTIA Security + Certification

Review and Approval Dates

Department Chair

03/04/2020

Dean

03/04/2020

Technical Review

03/10/2020

Curriculum Committee

03/10/2020

DTRW-I

03/11/2020

Curriculum Committee

03/25/2020

Board

3/25/2020

CCCCO

3/27/2020

Control Number

CCC000543436

DOE/accreditation approval date

MM/DD/YYYY