CNSE M56: COMPTIA ADVANCED SECURITY PRACTITIONER PREPARATION

Originator
egarcia

Co-Contributor(s)

Name(s)
Rickard, Kevin (krickard)
Bennington, Ruth (rbennington)
Davis, Howard (hdavis)

College
Moorpark College

Discipline (CB01A)
CNSE - Computer Netwrk Sys. Engr. Prg

Course Number (CB01B)
M56

Course Title (CB02)
CompTIA Advanced Security Practitioner Preparation

Banner/Short Title
CompTIA Advanced Security Prac

Credit Type
Credit

Start Term
Spring 2023

Catalog Course Description
Examines advanced security topics and use of security tools. Includes user access management, advanced storage, automation, networking, logging, software management and security administration tasks with heavy emphasis on applied security. Covers topics from Comptia Advanced Security Practitioner (CASP) certification exam.

Additional Catalog Notes
Prepares students for Comptia Advanced Security Practitioner certification exam.

Taxonomy of Programs (TOP) Code (CB03)
0708.00 - *Computer Infrastructure and Support

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)
B - Advanced 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
Will not be required

Grading method
(L) Letter Graded

Alternate grading methods
(O) Student Option- Letter/Pass
(P) Pass/No Pass Grading

Does this course require an instructional materials fee?
No

Repeatable for Credit
No

Is this course part of a family?
No

Units and Hours

Carnegie Unit Override
No

In-Class

Lecture
Minimum Contact/In-Class Lecture Hours
35
Maximum Contact/In-Class Lecture Hours
35

Activity

Laboratory
Minimum Contact/In-Class Laboratory Hours
52.5
Maximum Contact/In-Class Laboratory Hours
52.5

Total in-Class

Total in-Class
Total Minimum Contact/In-Class Hours
87.5
Total Maximum Contact/In-Class Hours
87.5

Outside-of-Class

Internship/Cooperative Work Experience

Paid

Unpaid

Total Outside-of-Class

Total Outside-of-Class
Minimum Outside-of-Class Hours
70
Maximum Outside-of-Class Hours
70

Total Student Learning

Total Student Learning
Total Minimum Student Learning Hours
157.5
Total Maximum Student Learning Hours
157.5

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

Advisories on Recommended Preparation
CNSE M55 and CNSE M82

Requisite Justification

Requisite Type
Recommended Preparation

Requisite
CNSE M55

Requisite Description
Course in a sequence

Level of Scrutiny/Justification
Closely related lecture/laboratory course

Requisite Type
Recommended Preparation

Requisite
CNSE M82

Requisite Description
Course in a sequence

Level of Scrutiny/Justification
Closely related lecture/laboratory course

Student Learning Outcomes (CSLOs)

	Upon satisfactory completion of the course, students will be able to:
1	set up user, root, and group account and policies; password policy, authentication methods, and configure file and directory permission.
2	implement transmission control program for network services such as networking, web services, remote access, and network security policies.
3	identify the various tools and processes security practitioners use to implement security solutions based on security risk and compliance goals.
4	practice using penetration testing and forensics analysis tools to assess system security including performing security tasks, and and reviewing security logs.

Course Objectives

	Upon satisfactory completion of the course, students will be able to:
1	configure and enable various network services related to internet protocol services.
2	configure and implement secure file sharing and system logging.
3	configure and enable Dynamic Host Configuration Protocol.
4	configure and implement web hosting.
5	enable and configure secure shell, crontab, and automation tasks.
6	configure and implement public key infrastructure.
7	implement extended file attributes.
8	implement and use sudo (superuser do).
9	demonstrate ability to integrate scripts such as Python and/or BASH.
10	configure log management services.
11	describe the internal and external security maintenance procedures.
12	demonstrate understanding key risk indicators that measure risk and compliance for cybersecurity readiness.
13	apply appropriate risk strategies given a set of security requirements.

Course Content

Lecture/Course Content

10% - Introducing Linux:

- Working on the Command Line
- Getting Help
- Editing Files

10% - Managing Group Accounts:

- Managing User Accounts
- Develop an Account Security Policy
- File Permissions

10% - Managing Local Storage: Essentials:

- Manage Local Storage: Advanced Features
- Manage Network Storage
- Develop a Storage Security Policy

15% - Automation:

- Crontab and at
- Scripting
- Common Automation Tasks
- Develop an Automation Security Policy

15% - Networking Basics:

- Network Configuration
- Network Service Configuration: Essential Services
- Network Service Configuration: Web Services
- Connecting to Remote Systems
- Develop a Network Security Policy

10% - Process Control:

- System Logging
- Red Hat-Based Software Management
- Debian-Based Software Management
- Overall system security risk posture
- Governance, Risk and Compliance

30% - Security:

- System Booting
- Password Cracking
- Exploit Frameworks
- Footprinting, Scanning
- Firewalls, Port Scanning
- Intrusion Detection
- Additional Security Tasks
- Protocol Analysis
- Web Interceptors
- Kali Linux Security Suite

Laboratory or Activity Content

10% - Operating System Installation:

- Installing CentOS
- Installing Ubuntu
- Installing Kali & using Security Tools
- Manage files
- Using shell features
- Compressing files

10% - Help:

- Getting help with man
- Getting help with info
- Edit files with the vim editor
- Troubleshooting Linux issues
- Configuring user notifications

5% - User Accounts:

- Manage group accounts
- Manage group administrators
- Manage user accounts

10% - Account Security:

- Secure user accounts
- Configure sudo
- Test the security of accounts
- Develop an account security policy
- Manage file permissions
- Manage special permissions
- Enable Access Control Lists
- Manage file attributes
- Monitor security issues

10% - File Systems:

- Manage encrypted filesystems
- Configure Logical Volumes
- Administer disk quotas
- Manage hard and soft links
- Configure Samba
- Administer NFS
- Manage iSCSI
- Backup a filesystem
- Develop a backup security policy

15% - Automation:

- Manage crontab
- Configure at commands
- Script projects
- Secure crontab and at
- Create an automation security policy

10% - Networking:

- Explore networking components
- Configure networking on CentOS
- Configure networking on Ubuntu
- Configure a BIND server
- Configure a Postfix server
- Administer procmail and Dovecot
- Configure and administer an Apache server
- Configure a proxy server
- Create an LDAP server
- Configure a FTP server
- Administer a SSH server

10% - System Security:

- Administer kernel security parameters
- Secure the system with TCP Wrappers
- Configure Network Time Protocol
- Create a networking security policy
- Manage system processes
- Display system information
- Manage log files
- Configure log rotation

10% - System Administration:

- Manage software packages with rpm, yum, dpkg, and apt
- Configure GRUB
- Manage the startup process

- Explore Common Vulnerabilities and Exposure reports

10% - Security Tools:

- Manage and secure legacy services
- Use probing tools, AirCrack Tool
- Scan the network, Nmap Tool
- Create a firewall to protect a system
- Implement NAT
- Scan the system to determine if it has been compromised, Volatility Tool
- Use IDS Tools
- Configure fail2ban
- Implement a VPN
- Encrypt files with gpg
- ExifTool
- Forensics, Sleuth Kit Tool
- Dynamic versus Static Linked application programs

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

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):

Individual projects
Objective exams
Problem-solving exams
Skills demonstrations
Skills tests or practical examinations
Classroom Discussion
Projects
Reports/Papers/Journals

Instructional Methodology

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

Audio-visual presentations
Case studies
Class activities
Class discussions
Collaborative group work
Computer-aided presentations
Distance Education
Group discussions
Instructor-guided interpretation and analysis
Instructor-guided use of technology
Internet research
Laboratory activities
Lecture
Small group activities

Describe specific examples of the methods the instructor will use:

Instructor will integrate a learning management system, e.g., Canvas, for supplemental support such as providing lab supplemental materials and whitepapers.

Lab: Instructor will provide instructions on lab exercises along with screen prints explaining detailed steps. Labs will include instructor's comments and observations for students to note while completing labs. Students will be expected to complete labs and be able to explain why specific configurations are being deployed. Students will submit labs that are automatically scored online and submit completion scores as evidence of completion using a learning management system (LMS), for example, Canvas or Blackboard. Labs will include using a virtualized environment to support Centos, Ubuntu Linux systems and Kali Linux security tool.

Representative Course Assignments

Writing Assignments

1. Document system configuration. An example would be testing and documenting configuration files for Domain Name Services (DNS), Dynamic Host Configuration Protocol (DHCP) and Apache web server to learn about common security activities and security requirements of Linux administrators.
2. Analyze security tools for securing environments. An example would be scripting assignments to support automating a set of system security administration tasks to improve security posture.
3. Research multiple Linux distributions, and security tools An example would be researching various Linux operating systems including Kali Linux to enhance student understanding of the need for differentiation between distributions due to a variety of security needs.
4. Review Security Enhanced Linux scripts and automation tools for securing environments.

Critical Thinking Assignments

1. Apply appropriate logic and syntax learned in class to use tools, and or scripts to solve and automate a given task or problem such as security audits, monthly reports, program logging and weekly rollups.
2. Enabe a secure shell connection to a remote server by researching components using Linux tools and web search to developing parameter choices and resolve security concerns.
3. Assess a web server for security controls to match website security objectives giving students the opportunity to think creatively and develop inquiries to discover additional or unknown information.

Reading Assignments

1. Review and explain the benefits of various Linux utilities and security tools that help with system administration or improve security.
2. Review in depth a specific Linux program or tool and how it improves system functionality, or solves a technical or business problem.
3. Review whitepapers and provide a short explanation of the benefit of this configuration.
4. Review prominent Linux documents such as Security Best Practices.

Skills Demonstrations

1. Demonstrate use of Kali Linux security tool and explain the various security features.
2. Configure the Linux system as required with necessary components and services that meet the technical requirements that satisfy either automation or security requirements.
3. Apply Security Best Practices given a Linux distribution.
4. Run security programs and scripts that identify security improvements.

Outside Assignments

Representative Outside Assignments

1. Utilize virtualization tools that provide students with additional knowledge and practice of the common day-to-day tasks of a Linux administrator.
2. Conduct field observations via online videos of network administration roles. For example, review interning, job shadowing, security job roles, or penetration testing to provide additional details to the day-to-day tasks of a Linux administrator.
3. Read assigned topics from the textbook and other sources such as books, periodicals, as well as informational and company websites that focus on Linux and Security.

Articulation

Equivalent Courses at other CCCs

College	Course ID	Course Title	Units
San Diego City College	INWT 205	CompTIA Advanced Security Practitioner (CASP) Certificatio Training	4
Coastline Community College	CST C230	CompTIA Advanced Security Practitioner	3
City College San Francisco	CNIT 125	Information Security Professional Practices	3

Attach Syllabus

CASP_CA_Community_Colleges.docx

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:
S2003

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

Area F: Ethnic Studies

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

Classic Textbook
Yes

Description
Abernathy, Robin and Troy McMillan. *CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide.* 2nd ed., Pearson IT Certification, 2018.

Resource Type
Textbook

Description
Lane, Nicholas, et al., *CASP+ CompTIA Advanced Security Practitioner Certification All-in-One Exam Guide (Exam CAS-003).* 2nd ed., McGraw-Hill, 2019.

Resource Type
Textbook

Classic Textbook
Yes

Description
Rothwell, William, and Denise Kinsey. *Linux Essentials for Cybersecurity*. Pearson IT Certification, 2018.

Resource Type
Textbook

Classic Textbook
Yes

Description
Rothwell, William. *Linux Essentials for Cybersecurity Lab Manual*. Pearson IT Certification, 2018.

Library Resources

Assignments requiring library resources
Research using library resources, specifically from the Safari O'Reilly database.

Sufficient Library Resources exist
Yes

Example of Assignments Requiring Library Resources
Research for a paper on topics such as modern security tools, modern threats and vulnerabilities.

Distance Education Addendum

Definitions

Distance Education Modalities
Hybrid (1%–50% online)
Hybrid (51%–99% 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)	Instructor will post a security related discussion question, students will respond to the question after performing some research. Students will also respond to other students responses.
E-mail	Instructor will email students with announcements about the course or an upcoming event. Students may email the instructor with their questions or concerns.
Face to Face (by student request; cannot be required)	Students will have the option to meet the instructor and work in the computer lab in the presence of the instructor to get one-on-one help from the instructor.
Other DE (e.g., recorded lectures)	Instructor may record lectures along with all zoo related transcripts and archive chat and post them on Canvas for students to view within a specified time frame.
Synchronous Dialog (e.g., online chat)	Instructor may be available on a certain day or days of the week within a certain time frame to help students and answer their questions via an online chat.
Telephone	Instructor may provide a phone number for the students where they can leave a voicemail and expect a call back within 24 hours.
Video Conferencing	Instructor may be available on a certain day or days of the week within a certain time frame to help students and answer their questions via live video conferencing.

Hybrid (51%–99% online) Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Other DE (e.g., recorded lectures)	Instructor may record the lectures and post them for students to view within a specified time frame to be ready for the accompanying assignments. Students will upload their assignment solutions to the course webpage.
Face to Face (by student request; cannot be required)	Students will have the option to meet the instructor and work in the computer lab in the presence of the instructor to get one-on-one help from the instructor.
Synchronous Dialog (e.g., online chat)	Instructor may be available on a certain day or days of the week within a certain time frame to help students and answer their questions via an online chat.
Video Conferencing	Instructor may be available on a certain day or days of the week within a certain time frame to help students and answer their questions via live video conferencing. Students may present their assignments or projects to the class and the instructor via live video conferencing.
Telephone	Instructor may provide a phone number for the students where they can leave a voicemail and expect a call back within 24 hours.
Asynchronous Dialog (e.g., discussion board)	Instructor will post an SLO related question and students will respond in a professional manner to the question as if presented during a job interview with both clarity and thoroughness of response. Students may also be asked to augment or respond to another students question.
E-mail	Instructor will email students with announcements about the course or an upcoming event. Students in turn may email the instructor with their questions or concerns. Students will email their assignments and projects to the instructor.

100% online Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Instructor will post an SLO related question and students will respond in a professional manner to the question as if presented during a job interview with both clarity and thoroughness of response. Students may also be asked to augment or respond to another students question.
E-mail	Instructor will email students with announcements about the course or an upcoming event. Students in turn may email the instructor with their questions or concerns. Students will email their assignments to the instructor.
Face to Face (by student request; cannot be required)	Students will have the option to meet the instructor and work in the computer lab in the presence of the instructor to get one-on-one help from the instructor.
Other DE (e.g., recorded lectures)	Instructor may record the lectures and post them for students to view within a specified time frame to be ready for the accompanying assignments. Students will upload their assignments to the course webpage.
Synchronous Dialog (e.g., online chat)	Instructor may be available on a certain day or days of the week within a certain time frame to help students and answer their questions via an online chat. Use of Zoom Break Rooms may be used to support online student collaboration.
Telephone	Instructor may provide a phone number for the students where they can leave a voicemail and expect a call back within 24 hours.
Video Conferencing	Instructor may be available on a certain day or days of the week within a certain time frame to help students and answer their questions via live video conferencing.

Examinations

Hybrid (1%–50% online) Modality

On campus
Online

Hybrid (51%–99% online) Modality

On campus
Online

Primary Minimum Qualification

COMPUTER INFORMATION SYS

Additional local certifications required

7+ years of Info Technology experience and working knowledge of Linux.

Review and Approval Dates

Department Chair

11/01/2021

Dean

11/02/2021

Technical Review

11/18/2021

Curriculum Committee

12/07/2021

DTRW-I

MM/DD/YYYY

Curriculum Committee
MM/DD/YYYY

Board
MM/DD/YYYY

CCCCO
MM/DD/YYYY

Control Number
CCC000602403

DOE/accreditation approval date
MM/DD/YYYY