GAVILAN COLLEGE
5055 Santa Teresa Blvd
Gilroy, CA 95023

Course Outline

COURSE: CSIS 179 DIVISION: 50 ALSO LISTED AS:

TERM EFFECTIVE: Fall 2021 CURRICULUM APPROVAL DATE: 5/11/2021

SHORT TITLE: INTRO TO INFO CYBERSEC

LONG TITLE: Introduction to Information Cybersecurity

Units	Number of Weeks	Type	Contact Hours/Week	Total Contact Hours
4	18	Lecture:	4	72
		Lab:	0	0
		Other:	0	0
		Total:	4	72

COURSE DESCRIPTION:

This course introduces students to network security concepts and prepares them for computer systems and network management duties. This course covers security concepts, communications and infrastructure security, basic cryptography, operational and organizational security, and legal and ethical issues. This course along with CSIS 184, 186, and 187; prepares you to take the professional industry CompTIA CySA+ certification exam. This course has the option of a letter grade or pass/no pass.

PREREQUISITES:

COREQUISITES:

CREDIT STATUS: D - Credit - Degree Applicable

GRADING MODES
- L - Standard Letter Grade
- P - Pass/No Pass

REPEATABILITY: N - Course may not be repeated

SCHEDULE TYPES:
- 02 - Lecture and/or discussion
- 05 - Hybrid
- 71 - Dist. Ed Internet Simultaneous
- 72 - Dist. Ed Internet Delayed

STUDENT LEARNING OUTCOMES:

By the end of this course, a student should:

1. Define information security in the context of local area networks, World Wide Web, wireless networks, and cell phones.

2. Define and identify malicious code and audit information security schemes to determine the relative security of a computer or a network.

3. Implement various security protocols such as anti-virus software firewalls and WEP for wireless networks by Hardening Systems.

4. Explain cryptographic strengths and vulnerabilities as used in VPN (virtual private networks) and other tunneling protocols.

CONTENT, STUDENT PERFORMANCE OBJECTIVES, OUT-OF-CLASS ASSIGNMENTS

Curriculum Approval Date: 5/11/2021

10 Hours

Content: Introduction to Information Cybersecurity -

Understanding the Importance of Information Cybersecurity

Preventing Data Theft

Avoiding Legal Consequences

Maintaining Productivity

Foiling Cyber Terrorism

Thwarting Identity Theft

Understanding Information Cybersecurity

Attacker Profiles Including Hackers, Crackers, Script, Kiddies, Spies Employees, Cyber Terrorists

Understanding Basic Attacks: Social Engineering, Password Guessing, Weak Keys, Mathematical Attacks, Birthday Attacks. Examining Identity Attacks, Man-in-the-Middle Attacks, Replay, TCP/IP Hijacking, Identifying Denial of Service Attacks

Understanding Malicious Code (Malware), Viruses, Worms, Logic Bombs, Trojan Horses, Back Doors

Student Performance Objectives: Explain the challenge of information cybersecurity and state why it is important. Identify information cybersecurity terminology and define who are the attackers. Explain the CompTIA Security+ exam. Explore career options for those interested in mastering cybersecurity skills.

20 Hours

Secure Network Infrastructure and Communications -

Disabling Nonessential Systems

Hardening Operating Systems: Applying Updates, Securing the File System

Hardening Applications: Hardening Servers, Hardening Data Repositories, Hardening Networks: Firmware Updates, Network Configuration-

Working with the Network Cable Plant: Coaxial Cables, Twisted-Pair Cables, Fiber-Optic Cables, Securing the Cable Plant

Securing Removable Media: Magnetic Media, Optical Media, Electronic Media, Keeping Removable Media Secure

Hardening Network Devices: Hardening Standard Network Devices, Hardening Communication Devices, Hardening Network Security Devices

Designing Network Topologies: Security Zones, Network Address Translation (NAT), Honeypots, Virtual LANs (VLANs)

Student Performance Objectives: Examine the threats and risks that a computer system faces by looking at both software-based attacks and attacks directed against the computer hardware. Examine the expanding world of virtualization and how virtualized environments are increasingly becoming the target of attackers.

Examine the steps for protecting systems by looking at steps that should be taken to harden the operating system, Web browser, Web servers, and how to protect from communications-based attacks. Explore the additional security software applications that should be applied to systems.

20 Hours

Content: Web Security -

Protecting E-mail Systems, How E-Mail Works, E-mail Vulnerabilities, E-mail Encryption, Examining World Wide Web Vulnerabilities, JavaScript, Java Applet, ActiveX, Cookies, Common Gateway Interface (CCI), Naming Conventions

Securing Web Communications, Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Hypertext Transport Protocol (HTTPS), Securing Instant Messaging

Handling File Transfer Protocol (FTP)

Securing Remote Access, Tunneling Protocols, Layer 2 Tunneling Protocol (L2TP), Authentication Technologies, Secure Transmission Protocols, Virtual Private Networks

(VPNs)

Protecting Directory Services, Securing Digital Cellular Telephony, Wireless Application Protocol (WAP), Wireless Transport Layer Security (WTLS), Hardening Wireless Local Area Networks

(WLAN), IEEE, .11 Standards, WLAN Components, Basic WLAN Security, Enterprise WLAN Security

Student Performance Objectives: Provide an overview of network security by examining some of the major weaknesses that are found in network systems. Examine the different categories of attacks and the methods of attacks that are commonly unleashed against networks today. Examine how to create a secure network through both network design and technologies and also how to apply network security tools to resist attacker.

17 Hours

Content: Security Management -

Understanding Computer Forensics

Forensics Opportunities and Challenges

Responding to a Computer Forensics Incident

Securing the Crime Scene, Preserving the Data

Establishing the Chain of Custody

Examining Data for Evidence

Hardening Security through New Solutions

Student Performance Objectives: Perform vulnerability assessments. Define risk and risk management and examine the components of risk management, and look at ways to identify vulnerabilities so that adequate

protections can be made to guard assets. Explore users? auditing privileges, auditing how subjects use those privileges, and monitoring tools and methods.

3 Hours

Content: Legal Issues and Ethics -

Cybercrime

Ethics

Student Performance Objectives: Discuss the legal frameworks; including duties of security, privacy issues, and law enforcement access issues related to cybercrimes. Discuss how the ethical framework enable and constrain security technologies and policies.

2 Hours

Final Exam

METHODS OF INSTRUCTION:

Lecture, Computer Demonstrations, Projects

OUT OF CLASS ASSIGNMENTS:

Required Outside Hours: 48

Assignment Description:

Read textook chapter and complete "quizlet".

Required Outside Hours: 72

Assignment Description:

Out of Class Assignments: Complete assigned homework, demonstrations, and hands-on projects and/or case projects.

Required Outside Hours: 24

Assignment Description:

Study for exams, final.

METHODS OF EVALUATION:

Problem-solving assignments

Percent of total grade: 35.00 %

Percent range of total grade: 25% to 40% Homework Problems, Quizzes, Exams

Skill demonstrations

Percent of total grade: 35.00 %

Percent range of total grade: 25% to 40% Hands-On Exams

Objective examinations

Percent of total grade: 30.00 %

Percent range of total grade: 25% to 40% Multiple Choice, True/False, Matching Items, Completion

REPRESENTATIVE TEXTBOOKS:

Wm. Arthur Conklin and Greg White and Chuck Cothren and Roger Davis and Dwayne Williams. Principles of Computer Security: CompTIA Security+ and Beyond , Fifth Edition. New York, NY: McGraw Hill,2018.

ISBN: 10: 1260026019; 13: 9781260026016

Reading Level of Text, Grade: 12+ Verified by: Ellen Venable

Recommended Other Texts and Materials

Security + Guide to Network Security Fundamentals, 7th Edition, 2021; Ciampa, Mark; Cengage Learning, Boston, MA

ARTICULATION and CERTIFICATE INFORMATION

Associate Degree:
CSU GE:
IGETC:
CSU TRANSFER:
Transferable CSU, effective 200830
UC TRANSFER:
Not Transferable

SUPPLEMENTAL DATA:

Basic Skills: N
Classification: Y
Noncredit Category: Y
Cooperative Education:
Program Status: 1 Program Applicable
Special Class Status: N
CAN:
CAN Sequence:
CSU Crosswalk Course Department:
CSU Crosswalk Course Number:
Prior to College Level: Y
Non Credit Enhanced Funding: N
Funding Agency Code: Y
In-Service: N
Occupational Course: C
Maximum Hours:
Minimum Hours:
Course Control Number: CCC000456075
Sports/Physical Education Course: N
Taxonomy of Program: 070810