***Gavilan College***

5055 Santa Teresa Blvd
Gilroy, CA 95023

***Course Outline***

**Course:** CSIS 179 Also Listed As:

**Term Effective:**Fall 2021 2015

**Short Title:** INTRO TO INFO CYBERSEC

**Long Title:** Introduction to Information Cybersecurity

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Units** | **Weeks** | **Type** | **Hours/Week** | **Total Contact Hours** |
| 4.00 | 18 | Lecture: | 4.00 | 72.00 |
|  | Lab: | 0.00 | 0.00 |
|  | Total: | 4.00 | 72.00 |

**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.

**Pre-requisite:** None

**Pre/Co-requisite:** None

**Corequisite:** None

**Advisory:** None

Unit Status: D - Credit - Degree Applicable

Grading Modes: Option of a standard letter grade or Pass/no pass

Repeatability: Course may not be repeated

**Methods of Instruction:**
Lecture, Computer Demonstrations, Projects

**Student Learning Outcomes:**
By the end of this course, a student should:

1. Identify the core principles of cybersecurity in the context of protecting networks, wireless networks, cell phones, and clients and servers.
2. Define and identify malicious code as generated by hackers, crackers, spies, and cyber terrorists.
3. Audit information security schemes to determine the relative security of a computer or a network.
4. Develop basic organizational security policies and the effectiveness of various cryptographic techniques and their impact on security.
5. Explain cryptographic strengths and vulnerabilities of Malware and Social Engineering.

**Course Content**

**Lecture Content:**

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

Content: 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

**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, midterm, 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

**Required 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 Representative Textbooks**
**Required Other Texts and Materials**

**Recommended Other Texts and Materials**

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