

CHT A162: FUNDAMENTALS OF INFORMATION SECURITY

Item	Value
Curriculum Committee Approval Date	10/20/2021
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	72 Total Hours (Lecture Hours 45; Lab Hours 27)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Open Entry/Open Exit	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

This course provides the fundamental knowledge necessary for a student to become proficient in the field of Information Security. This course will prepare the student for a wide variety of security responsibilities. The curriculum covers a wide range of security concepts, including General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography, and Operational and Organizational Security. This course covers CompTIA™s Security+ content and provides preparation for students seeking the CompTIA Security+ Certification. ADVISORY: CIS A110 or IT A110 or CIS A191 or IT A191. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Demonstrate in project format network attacks on information systems using network analyzer tools.
2. Demonstrate in project format the ability to use Network scanners such as Nmap and SuperScan to determine if a system is vulnerable to attack.

Course Objectives

- 1. Explain network access control systems and methodology. 2. Describe cryptography concepts, standards, and applications. 3. Perform telecommunications and network security activities. 4. Design and implement physical security measures. 5. Perform operations and security management practices. 6. Explain applications and systems development security techniques. 7. Describe risk mitigation techniques and how they apply to organization and individuals. 8. Describe ethical issues, pertinent laws, and how to conduct investigations.

Lecture Content

1. Network Security a. Explain the security function and purpose of network devices and technologies b. Apply and implement secure network administration principles c. Distinguish and differentiate network design elements and compounds d. Implement and use

common protocols e. Identify commonly used default network ports f. Implement wireless network in a secure manner 2. Compliance and Operational Security a. Explain risk related concepts b. Carry out appropriate risk mitigation strategies c. Execute appropriate incident response procedures d. Explain the importance of security related awareness and training e. Compare and contrast aspects of business continuity f. Explain the impact and proper use of environmental controls g. Execute disaster recovery plans and procedures h. Exemplify the concepts of confidentiality, integrity and availability (CIA) 3. Threats and Vulnerabilities a. Analyze and differentiate among types of malware b. Analyze and differentiate among types of attacks c. Analyze and differentiate among types of social engineering attacks d. Analyze and differentiate among types of wireless attacks e. Analyze and differentiate among types of application attacks f. Analyze and differentiate among types of mitigation and deterrent techniques g. Implement assessment tools and techniques to discover security threats and vulnerabilities h. Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning 4. Application, Data and Host Security a. Explain the importance of application security b. Carry out appropriate procedures to establish host security c. Explain the importance of data security d. Explain the function and purpose of authentication services e. Explain the fundamental concepts and best practices related to authentication, authorization and access control f. Implement appropriate security controls when performing account management 5. Access Control and Identity Management a. Explain the function and purpose of authentication services b. Explain the fundamental concepts and best practices related to authentication, authorization and access control c. Implement appropriate security controls when performing account management 6. Cryptography a. Summarize general cryptography concepts b. Use and apply appropriate cryptographic tools and products c. Explain the core concepts of public key infrastructure d. Implement PKI, certificate management and associated components

Lab Content

1. Malware and Social Engineering Attacks Block a USB Drive Scan for Rootkits Use a Software Keylogger 2. Application and Network Attacks Set Web Browser Security Hosts File Attack ARP Poisoning Create an HTTP Header 3. Vulnerability Assessment and Mitigating Attacks Using an Internet Port Scanner Using the GFI LANGuard Vulnerability Scanner Launching the Linux Wireshark Network Protocol Analyzer and Analyze Captured Traffic 4. Host, Application and Data Security Setting Windows Local Security Policy Viewing Windows Firewall Settings Viewing Logs Using Windows Event Viewer 5. Network Security Using Behavior Based Monitoring Tools Using an Internet Content Filter Configure Windows Client for Network Access Protection 6. Administering a Secure Network Using and FTPS Client Using a Faster/Safer DNS Install a Cloud Desktop Application View SNMP Management Information Base (MIB) Elements 7. Wireless Network Security Download and Install a Wireless Monitor Gadget Install and Use Vistumbler Substitute a MAC Address Using SMAC Install and Use a Virtual Router as an Evil Twin 8. Access Control Fundamentals Using Discretionary Acces Control to Delegate Authority in Windows Enabling IEEE 802.1x 9. Authentication and Account Management Download and Install a Password Management Application Using Cognitive Biometrics Create and use an OpenID Account 10. Basic Cryptography Running and RSA Cipher Demonstration Installing Command-Line and GUI Hash Generators and Comparing Hashes Using TrueCrypt 11. Advanced Cryptography Viewing Digital Certificates Viewing Digital Certificate Revocation Lists and Untrusted Certificates Downloading and Installing a Digital Certificate 12. Business Continuity Creating and Restoring a Disk Image Backup Entering and

Viewing Metadata Viewing Windows Slack and Hidden Data Scheduling a Backup Using Windows Server 2008 Backup and Allocating Disks 13. Risk Mitigation Online Ethics Training

years of professional experience, or any associate degree and six years of professional experience.

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Textbooks Resources

1. Required Ciampa, Mark. Comp TIA Security+ , 7th ed. Cengage Learning, 2020

Instructional Techniques

Lecture and application of ideas Students will be presented material from several different sources, including, but not limited to study guides, Web-based curriculum, in-class demonstrations of systems integration and personal experiences of industry professionals. Individual and paired exercises During the lab portion of the class, students will be required to perform many of the tasks of a network administrator. In order to complete several projects, students will need to work together in teams to build working local area networks. Interactive computer-based assignments Using computer and Web-based training tools, students will be working on simulated networks in order to solve problems.

Reading Assignments

45 hours (3hrs/wk) assigned from text

Writing Assignments

Program and configure a set of routers to create a simulated Wide Area Network (WAN) infrastructure. Given a minimum set of requirements, the student will design a recommended solution accommodating routing technologies using some combination of hardware and software. After the solution is designed, the student will create a presentation describing the results.

Out-of-class Assignments

45 hours (3hrs/wk). Student performance on quizzes, tests, including short essays, and laboratory assignments will be used to determine proficiency

Demonstration of Critical Thinking

Reading and writing assignments Web-based research Term or other paper(s) Laboratory reports Problem solving demonstrations Exams Homework problems Skill demonstrations Performance exams Case study presentations Objective examinations, including Multiple-choice True/false Completion

Required Writing, Problem Solving, Skills Demonstration

Program and configure a set of routers to create a simulated Wide Area Network (WAN) infrastructure. Given a minimum set of requirements, the student will design a recommended solution accommodating routing technologies using some combination of hardware and software. After the solution is designed, the student will create a presentation describing the results.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelor's degree and two