South Central College

COMP 2475 Security Basics

Course Outcome Summary

Course Information

Description An introduction to the various technical and administrative aspects of Information Security (INFOSEC), this course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system with appropriate intrusion detection and reporting features. Students will be exposed to a wide spectrum of security activities, methods, methodologies, and procedures. The terminal objectives for this course as defined in NSTISSI Training Standards 4011 are:
1. Understand the threats to and vulnerabilities of information systems
2. Recognize the need to protect data, information, and the means to process it
3. Develop a working knowledge of INFOSEC principles and practices
4. Design, execute, and evaluate INFOSEC security procedures and practices
(Prerequisites: COMP 1360)

Total Credits 4

Total Hours 64

Types of Instruction

Instruction Type	Credits/Hours
Lecture	4/64

Pre/Corequisites

COMP 1360

Institutional Core Competencies

Civic Engagement and Social Responsibility - Students will be able to demonstrate the ability to engage in the social responsibilities expected of a community member.

Communication - Students will be able to demonstrate appropriate and effective interactions with others to achieve their personal, academic, and professional objectives.

Critical and Creative Thinking - Students will be able to demonstrate purposeful thinking with the goal of using a creative process for developing and building upon ideas and/or the goal of using a critical process for the analyzing and evaluating of ideas.

Course Competencies

1. Explain the fundamental concepts of information security.

Learning Objectives

Define the key terms and critical concepts of information security.
Describe the purpose of information security and the CIA triad.
Explain how information security differs from computer security.
Explain principle of least privilege, defense-in-depth, and separation of duties.
Define threat agent, action, asset in the context of information security.
Explain the concepts of a kill-chain and the IT controls matrix.

2. Explain the security function and purpose of network devices and technologies and the proper use of these devices to design a secure network.

Learning Objectives

List the major protocols used for secure network communication.
Apply and implement secure network administration principles.
Demonstrate secure network design principles such as subnetting, segmenting, DMZ, and NAT.
List network-based tools capable of detecting an information security incident such as network vulnerability scanners, netflow monitoring, and network intrusion detection systems.

3. Identify and remediate common operating-system vulnerabilities.

Learning Objectives

Explain the challenges involved in patching systems and common approaches to patch management.
Explain the challenges in reducing user privileges and common approaches to privilege management.
List tools available for auditing operating-system security.
List host-based tools capable of detecting an information security incident such as file integrity monitoring and host intrusion detection systems.

4. Explain cryptography and implement cryptographic systems.

Learning Objectives

Summarize general cryptography concepts such as symmetric and asymmetric encryption, hashing, and non-repudiation.
Apply appropriate cryptographic tools, techniques, and procedures.
Explain the core concepts of public-key cryptography.
Explain cryptographic attacks such as replay, man-in-the-middle, side-channel attacks, and brute force attacks.
Remediate cryptographic attacks such as replay, man-in-the-middle, side-channel attacks, and brute force attacks.

5. Identify and remediate common application-layer vulnerabilities found in web applications.

Learning Objectives

Explain XSS, CSRF, SQLi, and other vulnerabilities present in many web applications.
Demonstrate ability to find these vulnerabilities in code or using pentesting tools.
Explain how to remediate common vulnerabilities present in many web applications.

6. Explain important state and federal laws regarding computer crime.

Learning Objectives

Summarize the Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Stored Communication Act, and the PATRIOT act.
Explain where to find State of Minnesota laws regarding computer crime.
Explain basic concepts of criminal law such as arrest, prosecute, convict, and the role of the 5th amendment.

7. Defend against offensive security techniques.

Learning Objectives

Describe the five phases of a malicious attack.
Demonstrate basic proficiency with tools for reconnaissance, scanning, and exploiting target systems.
Analyze and differentiate among types of malware.
Analyze and differentiate among types of attack.
Describe the tools, tactics, and procedures commonly used by attackers.

8. Explain the role that physical security plays in information security.

Learning Objectives

Describe how pin-and-tumbler and wafer locks work and how poor quality locks are defeated.
Describe three classes of fire and the appropriate way to attack such a fire.
Environmental Monitoring, HVAC, Incident Response and Computer Forensics.
Explain the role of the physical component of a comprehensive security program.
List the essential elements of physical access monitoring and control.

9. Develop a business continuity plan.

Learning Objectives

Explain the purpose of hot sites, cold sites, and warm sites.
Explain contingency planning and it's relationship to other business plans.
Explain IT service delivery and why the heck a security person cares about it.
Explain contingency planning and it's relationship to other business plans
Explain the impact of utility interruptions

10. Develop administrative security controls.

Learning Objectives

Describe the elements of policies, procedures, standards and guidelines.
Describe common information security policies.
Explain the importance of security related awareness and training.
Explain how an organization can institutionalize it's information security program.
Create information security policies.

11. Explain industry compliance and operational security.

Learning Objectives

Explain the concept of risk management and how it applies to selection of security controls.
Explain the difference between qualitative and quantitative risk management.
List common industry regulations that are applicable to business functions.
Implement appropriate risk mitigation strategies given a scenario.
Summarize the security implications of integrating systems and data with third parties.

12. Describe incident response and basic forensic procedures.

Learning Objectives

Collect forensic evidence from hard drives, network devices, and server logs.
Explain order of volatility and how it relates to forensic collection.
Summarize common incident response procedures.
Compose a complete incident response report.
Collect indicators of compromise.
Construct incident timeline of events.

SCC Accessibility Statement

South Central College strives to make all learning experiences as accessible as possible. If you have a disability and need accommodations for access to this class, contact the Academic Support Center to request and discuss accommodations. North Mankato: Room B-132, (507) 389-7222; Faribault: Room A-116, (507) 332-7222.

Additional information and forms can be found at: www.southcentral.edu/disability

This material can be made available in alternative formats by contacting the Academic Support Center at 507-389-7222.