Inver Hills Community College

ITC 2820: Information Systems Security Advanced

A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: 2

Lab Hours/Week: 2

OJT Hours/Week: *.*

Prerequisites:
ITC 2430 - Installation, Storage, and Compute with Windows AND ITC 2480 - Administering Linux Servers AND ITC 2530 - Enterprise Networking, Security, and Automation (Minimum grade: 2.0 GPA equivalent)

Corequisites: None

MnTC Goals: None

Focuses on the managerial aspects of information security and assurance. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. The course includes up-to-date information on changes in the field, such as national and international laws and international standards like the ISO 27000 series. Prerequisites: ITC 2430, ITC 2480, ITC 2530.

B. COURSE EFFECTIVE DATES: 08/26/2013 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

1. Introduction to the Management of Information Security (10%)
2. Planning for Security, Personnel and Law and Ethics (20%)
3. Planning for Contingencies (5%)
4. Information Security Policy (10%)
5. Developing the Security Program (5%)
6. Security Management Models (5%)
7. Security Management Practices (5%)
8. Risk Management: Identifying and Assessing Risk (25%)
9. Risk Management: Controlling Risk (5%)
10. Protection Mechanisms (15%)

D. LEARNING OUTCOMES (General)

1. Describe the role of an ethical hacker.
   Describe what you can do legally as an ethical hacker.
   Describe what you can't do as an ethical hacker.
   Describe the different types of malicious software.
   Describe methods of protecting against malware attacks.
   Describe the process of authentication
   Describe the types of network attacks
   Identify physical security attacks and vulnerabilities
2. Use Web tools for footprinting
   Conduct competitive intelligence
   Describe DNS zone transfers
   Identify the types of social engineering
   Describe port scanning and types of port scans
   Describe port-scanning tools
   Explain the function of ping sweeps
   Explain how shell scripting is used to automate security tasks
   Describe vulnerabilities of the Windows and Linux operating systems
3. Explain techniques to harden systems
   Identify vulnerabilities of embedded operating systems and best practices for protecting them
   Explain Web application vulnerabilities
   Describe the tools used to attack Web servers
   Explain wireless technology
   Describe wireless networking standards
   Describe the process of authentication
   Describe wardriving
   Describe wireless hacking and tools used by hackers and security professionals
   Summarize the history and principles of cryptography
4. Describe symmetric and asymmetric encryption algorithms
   Explain public key infrastructure (PKI)
   Describe possible attacks on cryptosystems
   Explain how routers are used as network protection systems
   Describe firewall technology and tools for configuring firewalls and routers
   Describe intrusion detection and prevention systems and Web-filtering technology
   Explain the purpose of honeypots
5. Students will practice business soft skills including written, active listening, and oral presentation.
   Students will document evidence of business skill practice in an electronic portfolio.

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted