Montgomery College
Germantown Campus
NW270: Information Security Capstone
Master Course Syllabus

Course Description:

Provides a review of methods for identifying network vulnerabilities, implementing network defense and exploring network forensics. Students will have opportunities to implement a layered defense on a practical network - including using tools to analyze the vulnerabilities of a network. Additionally, students will research products that could serve as countermeasures against potential attacks, implement security features of the network's operating systems and develop alternate solutions based upon cost and level of security required. The course also provides students with the practice skills necessary to enhance their existing network security background and prepare for Professional Security Certification(s)

Range of Subject Matter – Model Course Outline:

1. Security Trends
    a. Evolution of computing
    b. Information Warfare
    c. Hacking and Attacking
    d. Management
    e. Internet and Web Activities
    f. A Layered Approach
    g. Politics and Laws

2. Security Management Practices
    a. Fundamental Principles of Security - The CIA Triad
    b. Administrative, Technical and Physical Controls
    c. Roles & Responsibilities
    d. Change Control & Change Management
    e. Information Asset Management
    f. Security Architecture
    g. Risk Management Principles, Tools, Methodologies and Standards
    h. Policies, Standards, Guidelines & Procedures
    i. Data Classification
    j. Employment Policies and Practices
    k. Security Awareness Training
    l. Security Management Planning
    m. Information Systems Audit

3. Access Control
    a. Security Principles
    b. Identification and Authentication Techniques
    c. Access Control Models
    d. Access Control Techniques and Technologies
    e. Access Control Administration
    f. Access Control Types
    g. Access Control Monitoring

h. Passwords, One-Time Passwords, Tokens, SmartCards, Biometrics
i. Access Control Techniques
j. Data Ownership and Custodianship

4. Security Models and Architecture
    a. Platform Architectures
    b. Computer & Network Architectures
    c. Operating System Principles / Architectures
    d. Threats to Shared Environments
    e. Trusted Systems
    f. Reference Monitors & Kernels, TCB
    g. Operating Modes
    h. Security Models
    i. State Machine Models
    j. Biba Matrix
    k. Bell-LaPadula Matrix
    l. Clark-Wilson
    m. Certification & Accreditation
    n. TCSEC, ITSEC, Common Criteria

5. Physical Security
    a. Planning Process
    b. Facilities Management
    c. Physical Security Risks
    d. Physical Security Component Selection Process
    e. Environmental Issues
    f. Administrative Controls
    g. Media Storage Requirements
    h. Layered Physical Defense and Entry Points
    i. Perimeter Security: Fence, lighting, surveillance devices

6. Telecommunications and Networking Security
    a. Open System Interconnect Model
    b. TCP/IP
    c. Types of Transmission
    d. Network Topology
    e. LAN Media Access Technologies
    f. Protocols
    g. Networking Devices
    h. Network Segregation and Isolation
    i. Networking Services
    j. Intranets and Extranets
    k. Metropolitan Area Network
    l. Wide Area Network
    m. Remote Access
    n. Network and Resource Availability
    o. Cabling and data transmission types
    p. TEMPEST
    q. Wireless Technologies

7. Cryptography
    a. History of Cryptography
    b. Cryptography Definitions
    c. Strength of the Cryptosystem
    d. Goals of Cryptosystems
    e. Hybrid Cryptosystems
    f. Methods of Encryption: Hash Functions / Message Digests & Message Authentication Codes
    g. Public Key Infrastructure (PKI)
    h. Types of Ciphers: Stream vs Block Ciphers / Symmetric Ciphers, Public-Key Ciphers
    i. Digital Certificates and PKI
    j. Digital Signatures
    k. SSL / SSH
    l. Steganography
    m. E-mail / Internet Security
    n. Non-repudiation

8. Business Continuity Planning
    a. Business Continuity and Disaster Recovery
    b. Make It Part of the Security Policy and Program
    c. Business Impact Analysis
    d. Business Continuity Planning Requirements
    e. End-User Environment
    f. Backup Alternatives
    g. Choosing a Software Backup Facility
    h. Recovery and Restoration
    i. Testing and Drills
    j. Emergency Response

9. Law, Investigation, and Ethics
    a. Facets of Cyberlaw
    b. Computer Ethics
    c. Well-Known Computer Crimes
    d. Identification, Protection, and Prosecution
    e. Types of Laws
    f. Discarding Equipment and Software Issues
    g. Computer Crime Investigations
    h. Import and Export Laws
    i. Privacy
    j. National/International Cooperation Efforts
    k. Intellectual Property: Trade Secrets, Patents, Copyright
    l. Incident Response
    m. Investigation Process
    n. Computer Forensics
    o. Rules of Evidence & Legal Proceedings

10. Application and System Development
    a. Introduction; Changes in the Environment
    b. Threat Agents: Hackers, crackers, and virus authors
    c. Vulnerabilities

d. Mobile Code: Agents, applets, ActiveX, Java
e. Buffer Overflows, Stack Smashing, etc.
f. Malicious Code & Logic: Viruses, Trojans, Worms & Logic Bombs
g. Databases, Data Warehousing & Knowledge-based Systems
h. System Development Life Cycle
i. SDLC Phases
j. Iterative Development Models
k. Programming Languages and Translators
l. Object Oriented Design and Programming
m. Data Types, Format, and Length
n. Security Features of Languages
o. Implementation and Default Issues
p. Mobile Code
q. Failure States
r. Safeguards, Mitigation and Controls
s. Attacks: Code alteration, flooding, salami, SQL injection, trapdoors, DoS, etc.

11. Operations Security
    a. Operating System Architecture
    b. Principles of Privilege: Need-to-know, Least Privilege, Rotation of Duties & Separation of Duties
    c. Due Care & Due Diligence
    d. Privacy and Protection
    e. Sensitive Information and Media
    f. Media Controls
    g. Media, Backups and Change Control Management
    h. Personnel Controls
    i. Infrastructure Controls
    j. Configuration Management and Contingency Management
    k. Audit Trails & Reporting
    l. Threats & Countermeasures
    m. Violations, Breaches and Reporting

Instructional Materials:

Required Textbook: CISSP Exam Cram, 2nd Edition by Michael Gregg, Publisher: Pearson IT Certification, ISBN-13: 978-0-7897-3806-6
Recommended Textbook: CISSP All-in-One Exam Guide, Fifth Edition by Shon Harris, Publisher: McGraw-Hill Osborne Media, ISBN-13: 9780071602174.

Evaluation:

Team Exercise - 15 Points
Tests - 10 Points
Labs - 20 Points
Online Discussions - 30 Points
Final Exam - 25 Points