Course Description

This course provides a comprehensive introduction of network security, its use and implementation. Students will be introduced to general security, communication security, infrastructure security, cryptography, operational/organizational security and physical security. Students will gain practical skills and learn techniques of detecting and correcting security vulnerabilities. Students are expected to complete several assignments preparing to CompTIA professional security certification.

Prerequisites

Basic skills- ENG 095; ESL 095; ACR 095; MAT 012/051; CIS 345 (Telecommunication Networks I) or departmental approval

Learning Outcomes and Assessment

After completing this course, students will be able to:

- **Outcome:** Identify the physical security and its properties and uses
  **Assessment:** Lab exercises and homework
- **Outcome:** Detect, prevent and recover intrusion
  **Assessment:** Lab exercises homework and exam questions
- **Outcome:** Explain the cryptography and its different types
  **Assessment:** Home work, short essays and exam questions
- **Outcome:** Discover and correct vulnerabilities in forensics, attacks and malicious codes
  **Assessment:** Lab exercises, homework and exam questions
- **Outcome:** Configure and manage disaster recovery and ensure business continuity
  **Assessment:** Lab exercises, case study project and exam questions

General Education Outcomes and Assessment

- **Quantitative Skills** – Students will use quantitative skills and concepts and methods of mathematics to solve problems
  **Assessment:** Use formulas, graphs and concepts of mathematics to solve problems in security assignments
- **Information and Technology Literacy** – Students will collect, evaluate and interpret information and effectively use information technologies
  **Assessment:** Use security hardware and software to complete assignments and lab exercises

Required Text & Readings

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Author:</td>
<td>Ciampa, Mark</td>
</tr>
<tr>
<td>Publisher:</td>
<td>Course Technology</td>
</tr>
</tbody>
</table>

Other Resources

Flash drives and CDs are needed for use during Lab.

Use of Technology (if applicable)

Evaluation & Requirements of Students

First Exam 25%
Outline of Topics:

   - Objective: Define, specify or identify examples of Essential Security Practices
   - Best/good security practices
   - Security policy and procedure Implementation

2. Security Fundamentals
   - Objective: Identify or explain examples of risk management fundamentals and the basic tenets of IT security
   - Social engineering and countermeasures
   - Risk measurement fundamentals
   - Function and use of vulnerability assessment tools
   - Physical security basics
   - Security threats and principles (basics)

3. Administration & Maintenance Fundamental
   - Objective: Explain, identify or recognize essential operating system security practices
   - Understand hardening, blocking and patching at the platform level
   - Basics of file directory management

4. Administration & Maintenance Fundamentals
   - Objective: Describe, recognize or select good administrative maintenance and change-control issues and tools
   - Understanding default settings and their weaknesses
   - Fundamental maintenance policies and procedures

5. Authentication Fundamentals
   - Objective: Identify, specify or describe good access control and authentication process and techniques
   - Essential access control practices
   - Basic user authentication methodologies

6. Cryptography Basics
   - Objective: Identify key issues of cryptography, and be able to recognize basic cryptographic methods in use today
   - Understand secret key, public key, one-way hash functions

7. PKI and Digital Certificates
   - Objective: Explain, identify or recognize basic users, requirements and functions of PKI and digital certificates
   - Fundamentals of using, managing certificates
   - Understand basic strengths, weaknesses, and purpose of PKI and digital certificates

8. Malicious Code Fundamentals
   - Objective: Identify and explain malicious code threat and defense mechanisms
   - Understanding of viruses, worms, trojans
   - Essential-level familiarity of malicious code tools and defense tactics

   - Objective: Describe, recognize or select good intrusion detection methodologies, applications and disaster recovery practices
   - IDS basics, including methodologies and applications
   - Essential forensics procedures
   - Basic disaster recovery methods

10. Configuration fundamental Firewall Management Fundamentals
    - Objective: Describe, recognize or select good firewall architectures, properties and administration basics
    - Firewall administration procedures
    - Essential firewall architectures and properties (understanding or architectures).
11. Law, Ethics and Policy
   • Objective: Identify, specify or describe computer and network ethical, legal and privacy issues
   • Basics of rights and privileges in the corporate environment
   • Ethical IT Practices
   • Fundamental privacy requirements and legal usage of corporate, personal data

12. Devices
   • Objective: Identify, specify or describe computer and network devices.
   • Routers and Switches
   • Wireless
   • RAS
   • Telecom/PBX

13. TCP/IP Networking Fundamentals
   • Objective: Describe, recognize or select basic weaknesses in TCP/IP networking
   • TCP/IP & router fundamentals
   • Basic TCP/IP weaknesses

14. Design & Configuration Basics
   • Objective: Identify the security issues associated with system/network design and configuration
   • Network architecture basics

College Attendance Policy:

At BMCC, the maximum number of absences is limited to one more hour than the number of hours a class meets in one week. For example, you may be enrolled in a three-hour class. In that class, you would be allowed 4 hours of absence (not 4 days). In the case of excessive absences, the instructor has the option to lower the grade or assign an F or WU grade.

Academic Adjustments for Students with Disabilities:

Students with disabilities who require reasonable accommodations or academic adjustments for this course must contact the Office of Services for Students with Disabilities. BMCC is committed to providing equal access to all programs and curricula to all students.

BMCC Policy on Plagiarism and Academic Integrity Statement:

Plagiarism is the presentation of someone else’s ideas, words or artistic, scientific, or technical work as one’s own creation. Using the idea or work of another is permissible only when the original author is identified. Paraphrasing and summarizing, as well as direct quotations, require citations to the original source. Plagiarism may be intentional or unintentional. Lack of dishonest intent does not necessarily absolve a student of responsibility for plagiarism.

Students who are unsure how and when to provide documentation are advised to consult with their instructors. The library has guides designed to help students to appropriately identify a cited work. The full policy can be found on BMCC’s web side, www.bmcc.cuny.edu. For further information on integrity and behavior, please consult the college bulletin (also available online).