CS 325 Information Security  
Westminster College – Spring 17/18  
Tuesday/Thursday 11 – 12:30

Instructor:  Kelly Hartner  
Office: Hoyt 170  
E-mail: khartner@westminster.edu  
Phone: 724-946-7026  
Office Hours: MW 12:00-1:00 or by appointment

Course Description: This course looks at management issues and practical implications related to securing information systems. This course focuses on the Threat Environment, security Policy and Planning, Cryptography, Secure Networks, Access Control, Firewalls, Host Hardening, Application Security, Data Protection, Incident Response, and Networking and Review of TCP/IP. A clear theoretical understanding supports a large practical component where students learn to audit information systems and use contemporary security software.

This course provides the foundation for understanding the key issues associated with protecting information assets, determining levels of protection and response to security incidents and designing reasonable security measures for the protection of computer and network-stored data.

Objectives: In this course we will touch and explore various aspects of computer and network security. The goal is to lay a foundation for an understanding of how computer and network-stored data is vulnerable and what measures can be taken to protect it. Methodologies and procedures for the inspection, detection and reaction to security incidents will also be covered.

1. Articulate key security concepts related to IT security so that a layperson in the IT field could easily understand.
2. Demonstrate many security-related skills such as how to secure a network against a specific type of threat.
3. Demonstrate the ability to utilize resources to research security-related problems and resolutions.
4. Understand and evaluate current security-related issues.
5. Make intelligent, reasonable, thoughtful, and accurate decisions about IT security, vulnerabilities, and legal issues.

Text: Corporate Computer Security, 4/e  
Randall J. Boyle | Raymond R. Panko  

Structure: You should read the materials assigned for a particular class before coming to class. The D2L course page will be used to post slides and handouts. The College’s email system will be used to send announcements. Please read your email and check D2L on a regular basis.

Topics: The tentative schedule is attached. The instructor reserves the right to make changes.

Grading:  
<table>
<thead>
<tr>
<th>Assignment Type</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 assignments, 8 @ 20 points</td>
<td>160</td>
</tr>
<tr>
<td>10 quizzes, 10 @ 10 points</td>
<td>100</td>
</tr>
<tr>
<td>3 examinations, 2 @ 45 and 1 @ 60 points each</td>
<td>150</td>
</tr>
<tr>
<td>Group Project</td>
<td>75</td>
</tr>
<tr>
<td>Individual Project</td>
<td>25</td>
</tr>
<tr>
<td>Class participation &amp; attendance</td>
<td>25</td>
</tr>
<tr>
<td>Total</td>
<td>535</td>
</tr>
</tbody>
</table>

Typically, the grading scale is: 92-100% = A; 89 - 91.9=A-; 88-88.9 % = B+ and so on. However, I reserve the right to change the scale depending on how the final grades break.

Policy: Assignments are due at the start of the class. Late assignments are penalized by 10% immediately and an additional 5% for every class period up to one week past the due date. Assignments more than one week past the due
date are not accepted. Examinations and quizzes must be taken during the scheduled class period unless prior arrangements have been made or in documented emergencies. Incomplete grades are given only in rare circumstances and only by prior arrangement with the instructor.

If you miss a class, please see a classmate to get the notes. I'm happy to talk to you, but not willing to repeat my lecture!

Class attendance is important to your understanding of the materials presented and you should make every effort to attend class. This is a project-based course and your participation is CRUCIAL. You will be expected to contribute to the class discussion and work! Please feel free to stop by during office hours or at other times.

Occasionally, you may be asked to attend an event outside of class time. You will be informed about these activities as they occur.

Academic Integrity: Academic integrity is central to the purpose of any academic community. Please read the section in the catalog entitled "Academic Integrity." Of special concern is the issue of plagiarism, which is defined as leading your reader or listener to believe that what you have written or said is your own work, when, in fact, it is not. The range of plagiarism includes word-for-word copying of another's text without quotation marks and appropriate citation, to inappropriate paraphrasing of another's text, to even the unattributed borrowing of apt phrases or terms. All of these degrees of plagiarism are equally unethical and may be penalized with failure for the assignment, or, in extreme cases, failure for the course. Turn-it-in.com may be used during this course.

Assistance: If you are having problems with this course, or any other, Westminster College provides several sources of help: 1) The Learning Center (extension 6700), 2) Disability Resources (extension 7192), and 3) Counseling Services (extension 7340).
<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Goals and Objectives</th>
<th>Assignments/Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/16 – 1/18</td>
<td><strong>Introduction and Syllabus Discussion, Ch. 1: The Threat Environment</strong>&lt;br&gt;- Define the term threat environment.&lt;br&gt;- Use basic security terminology.&lt;br&gt;- Describe threats from employees and ex-employees.&lt;br&gt;- Describe threats from malware writers.&lt;br&gt;- Describe traditional external hackers and their attacks, including break-in processes, social engineering, and denial-of-service attacks.&lt;br&gt;- Know that criminals have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation.&lt;br&gt;- Distinguish between cyberwar and cyberterror.</td>
<td>T(1/16): Read Ch. 1 for R(1/18)&lt;br&gt;R(1/18): Lecture Chapter 1</td>
</tr>
<tr>
<td></td>
<td>1/23 – 1/24</td>
<td><strong>Ch. 2: Planning and Policy</strong>&lt;br&gt;- Justify the need for formal management processes.&lt;br&gt;- Explain the plan–protect–respond security management cycle.&lt;br&gt;- Describe compliance laws and regulations.&lt;br&gt;- Describe organizational security issues.&lt;br&gt;- Describe risk analysis.&lt;br&gt;- Describe technical security infrastructure.&lt;br&gt;- Explain policy-driven implementation.&lt;br&gt;- Know governance frameworks.</td>
<td>T(1/23): Lecture Chapter 1&lt;br&gt;R(1/24): Quiz – Chapter 1 Review&lt;br&gt;R(1/24): &quot;Sign&quot; non-hacking agreement&lt;br&gt;R(1/24): Start A1 in class due R(2/1)&lt;br&gt;R(1/24): Read Ch. 2 for R(1/30)</td>
</tr>
<tr>
<td>2</td>
<td>1/30 – 2/1</td>
<td><strong>Ch. 2: Planning and Policy (continued)</strong>&lt;br&gt;- Explain the concept of cryptography.&lt;br&gt;- Describe symmetric key encryption and the importance of key length.&lt;br&gt;- Explain the negotiation stage.&lt;br&gt;- Explain initial authentication, including MS-CHAP.&lt;br&gt;- Describe keying, including public key encryption.&lt;br&gt;- Explain how electronic signatures, including digital signatures, digital certificates, and key-hashed message authentication codes (HMACs), work.&lt;br&gt;- Describe public key encryption for authentication.&lt;br&gt;- Describe quantum security.&lt;br&gt;Explain cryptographic systems including VPNs, SSL, and IPsec.</td>
<td>T(1/30): Start A2 due R(2/8)&lt;br&gt;T(1/30): Lecture Chapter Two&lt;br&gt;R(2/1): A1 due&lt;br&gt;R(2/1): Lecture Chapter Two</td>
</tr>
<tr>
<td>3</td>
<td>2/6 – 2/8</td>
<td><strong>Ch. 3: Cryptography</strong>&lt;br&gt;- Explain the concept of cryptography.&lt;br&gt;- Describe symmetric key encryption and the importance of key length.&lt;br&gt;- Explain the negotiation stage.&lt;br&gt;- Explain initial authentication, including MS-CHAP.&lt;br&gt;- Describe keying, including public key encryption.&lt;br&gt;- Explain how electronic signatures, including digital signatures, digital certificates, and key-hashed message authentication codes (HMACs), work.&lt;br&gt;- Describe public key encryption for authentication.&lt;br&gt;- Describe quantum security.&lt;br&gt;Explain cryptographic systems including VPNs, SSL, and IPsec.</td>
<td>T(2/6): Quiz – Chapter 2 Review&lt;br&gt;T(2/6): Lecture Chapter Three&lt;br&gt;T(2/6): Read Ch. 3 for R(2/8)&lt;br&gt;R(2/8): A2 due&lt;br&gt;R(2/8): Lecture Chapter Three</td>
</tr>
<tr>
<td>Week</td>
<td>Topics</td>
<td>Goals and Objectives</td>
<td>Assignments/Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
</tbody>
</table>
| 6     | 2/20 Ch. 3: Cryptography (continued) | T(2/20): Quiz – Chapter 3 Review  
T(2/20): Review for Exam 1  
R(2/22): Exam 1  
R(2/22): Read Ch. 4 for T(2/27)  
R(2/22): A3 Due |
| 7     | 2/27 Ch. 4: Secure Networks    | T(2/27): Start A4 Due R(3/15)  
T(2/27): Lecture Chapter Four  
R(3/1): Lecture Chapter Four |
| 8     | 3/6 Spring break – no classes  | T(3/13): Quiz – Chapter 4 Review  
T(3/13): Read Ch. 5 for R(3/15)  
T(3/13): Lecture Chapter Five  
R(3/15): Lecture Chapter Five  
R(3/15): A4 Due |
| 9     | 3/13 Ch. 5: Access Control     | T(3/20): Start A5 Due R(4/5)  
R(3/20): Quiz – Chapter 5 Review  
T(3/20): Lecture Chapter Six  
R(3/22): Lecture Chapter Six |
<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Goals and Objectives</th>
<th>Assignments/Schedule</th>
</tr>
</thead>
</table>
| 11   | Ch. 6: Firewalls | - Define firewalls in general (basic operation, architecture, and the problem of overload).  
- Describe how static packet filtering works.  
- Explain stateful packet inspection (SPI) for main border firewalls.  
- Describe how network address translation (NAT) works.  
- Explain application proxy firewalls and content filtering in SPI firewalls.  
- Distinguish between intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).  
- Describe antivirus filtering.  
- Define firewalls in general (basic operation, architecture, and the problem of overload).  
- Describe how static packet filtering works.  
- Explain stateful packet inspection (SPI) for main border firewalls.  
- Describe how network address translation (NAT) works.  
- Explain application proxy firewalls and content filtering in SPI firewalls.  
- Distinguish between intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).  
T(3/27): Quiz – Chapter 6 Review  
T(3/27): In class work time  
R(3/29): No class – Easter break |
| 12   | 4/3: No Class | - Define the elements of host hardening, security baselines and images, and systems administration.  
- Know important server operating systems.  
- Describe vulnerabilities and patches.  
- Explain how to manage users and groups.  
- Explain how to manage permissions.  
- Know Windows client PC security, including centralized PC security management.  
- Explain how to create strong passwords.  
- Describe how to test for vulnerabilities. | T(4/3): No class – Monday classes meet  
R(4/5): Review for Exam 2  
R(4/5): A5 Due |
| 13   | 4/10: Exam 2  
Ch. 7: Host Hardening and Ch. 8: Application Security | | T(4/10): Exam 2  
T(4/10): Read Ch. 7 and 8 for R(4/12)  
R(4/12): A6 Due  
R(4/12): Lecture Chapter 7 and 8 |
<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Goals and Objectives</th>
<th>Assignments/Schedule</th>
</tr>
</thead>
</table>
| 13   | Ch. 7: Host Hardening and Ch. 8: Application Security | • Explain why attackers increasingly focus on applications.  
• List the main steps in securing applications.  
• Know how to secure WWW services and e-commerce services.  
• Describe vulnerabilities in web browsers.  
• Explain the process of securing e-mail.  
• Explain how to secure voice over IP (VoIP).  
• Describe threats from Skype VoIP service.  
• Describe how to secure other user applications.  
• Know how to secure TCP/IP supervisory applications. | T(4/17): Lecture Chapter 7 and 8  
R(4/19): Lecture Chapter 7 and 8  
R(4/19): Start A7 |
| 14   | Ch. 9: Data Protection and Ch. 10: Incident and Disaster Response | • Explain the necessity for backup.  
• Describe backup scope and methods.  
• Describe the different RAID (redundant array of independent disks) levels.  
• Explain the need for data storage policies.  
• Explain database protections.  
• Explain the need for database access controls, auditing, and encryption.  
• Describe the difference between data leakage and data theft.  
• Explain data deletion, destruction, and disposal.  
• Explain digital rights management (DRM) and how it can prevent data loss.  
• Explain the basics of disaster response.  
• Describe the intrusion response process for major incidents.  
• Describe legal considerations.  
• Explain the necessity of backup.  
• Describe the functions and types of intrusion detection systems (IDSs).  
• Explain the importance of education, certification, and awareness.  
• Describe business continuity planning.  
• List the advantages of data centers.  
• Know the IT disaster recovery process. | T(4/24): Quiz – Chapter 7&8 Review  
T(4/24): Lecture Chapter 9 and 10  
T(4/24): Read Ch. 9 and 10 for R(4/26)  
R(4/26): A7 Due  
R(4/26): Lecture Ch. 9 and 10  
R(4/26): Start A8 Due R(5/3) |
| 16   | Review and Exam 3 for Chapters 7,8,9,10 | | T(5/1): Quiz – Chapter 9 & 10 Review  
T(5/1): Exam 3 Review  
R(5/3): A8 due  
R(5/3): Exam 3 |
<p>| Final | Group Presentations | Tuesday May 10 | 8:00 a.m to 10:30 a.m. | Group Presentations |</p>
<table>
<thead>
<tr>
<th>Assignment</th>
<th>Description</th>
<th>Rubric: Meets Expectations if ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assignment One (A1)</strong> &lt;br&gt; HOP1: Project 1 (pg. 51) &lt;br&gt; HOP1: Project 2 (pg. 51)</td>
<td>• Describe why article interests you &lt;br&gt; • Include facts from reading and lecture &lt;br&gt; • Nmap port scanner exercise &lt;br&gt; • Review current security sections of eWeek.com, The Register or Computer World. Apply reading selection, in class lecture and discussion, online interaction and course-related activities</td>
<td>• Clearly and concisely describes the what, why and how of the project. &lt;br&gt; • Follow Project 1 and Project 2 instructions in text to create a clear and concise document to be submitted to the A1 dropbox. &lt;br&gt; • Follow any other assignment instructions. &lt;br&gt; • Submitted on time.</td>
</tr>
<tr>
<td><strong>Assignment Two (A2)</strong> &lt;br&gt; HOP2: Project 1 (pg. 117) &lt;br&gt; HOP2: Project 2 (pg. 118)</td>
<td>• Review SANS website for important security problems, careers in security, read a white-paper, review templates for security policy writing. &lt;br&gt; • Refog keylogger exercise</td>
<td>• Clearly and concisely describes the what, why and how of the project. &lt;br&gt; • Follow Project 1 and Project 2 instructions in text to create document to be submitted to the A2 dropbox. &lt;br&gt; • SANS review summary will be clear, concise, applicable and meaningful &lt;br&gt; • Follow any other assignment instructions. &lt;br&gt; • Submitted on time.</td>
</tr>
<tr>
<td><strong>Assignment Three (A3)</strong> &lt;br&gt; HOP3: Project 1 (pg. 179) &lt;br&gt; HOP3: Project 2 (pg. 232)</td>
<td>• AxCrypt encryption exercise &lt;br&gt; • Enigma exercise</td>
<td>• Clearly and concisely describes the what, why and how of the project. &lt;br&gt; • Follow Project 1 (pg. 179) and Project 2 (pg. 232) instructions in text to create document to be submitted to the A3 dropbox. &lt;br&gt; • Follow any other assignment instructions. &lt;br&gt; • Submitted on time.</td>
</tr>
<tr>
<td>Assignment</td>
<td>Description</td>
<td>Rubric: Meets Expectations if ...</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Assignment Four (A4)</strong></td>
<td>HOP4: Project 1 Do NOT do HOP4: Project 2 (pg. 232) HOP4: Ping and Arp exercise - found in CS325 general files in D2L</td>
<td>- HTTPS web browsing • Clearly and concisely describes the what, why and how of the project. • Follow Project 2 instructions in text to create document to be submitted to the A4 dropbox. • Follow any other assignment instructions. • Submitted on time.</td>
</tr>
<tr>
<td><strong>Assignment Five (A5)</strong></td>
<td>HOP5: Project 1 (pg. 298) HOP5: Project 2 (pg. 299)</td>
<td>- Password Auditing – John the Ripper • Password Cracking • Clearly and concisely describes the what, why and how of the project. • Follow Project 1 and Project 2 instructions in text to create document to be submitted to the A5 dropbox. • Follow Project 2 instructions in text to • Follow any other assignment instructions. • Submitted on time.</td>
</tr>
<tr>
<td><strong>Assignment Six (A6)</strong></td>
<td>HOP6: Project 1 Do NOT do HOP6: Project 2 (pg. 360) HOP6: AD and Directory rights exercise - found in CS325 general files in D2L</td>
<td>- Windows Advanced Firewall • Clearly and concisely describes the what, why and how of the project. • Follow Project 2 instructions in text to create document to be submitted to the A6 dropbox. • Follow any other assignment instructions. • Submitted on time.</td>
</tr>
<tr>
<td><strong>Assignment Seven (A7)</strong></td>
<td>HOP7: Project 1 (pg. 416) HOP7: Project 2 (pg. 416)</td>
<td>- Windows event viewer exercise • Clearly and concisely describes the what, why and how of the project. • Follow Project 1 and Project 2 instructions in text to create document to be submitted to the A7 dropbox. • Follow any other assignment instructions. • Submitted on time.</td>
</tr>
<tr>
<td>Assignment</td>
<td>Description</td>
<td>Rubric: Meets Expectations if …</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Assignment 8 (A8)   | • File shredder exercise  
                     • Recuva exercise                                                             | • Clearly and concisely describes the what, why and how of the project.  
                     • Follow Project 2 (pg. 521) and Project 2 (pg. 575) instructions in text to  
                       create document to be submitted to the A8 dropbox.  
                     • Follow any other assignment instructions.  
                     • Submitted on time.                                                                 |
| HOP8: Project 2 (pg. 521) |                                                                             |                                                                                                   |
| HOP8: Project 2 (pg. 575) |                                                                             |                                                                                                   |
| Group Project       | • Each group will create a company and design, a security plan, including policy, risk assessment and remediation, etc. | • The complete case study will be submitted in a written report.  
                     • A summary of the case study will be presented to the class.                                                                 |
| Individual Case Study | • Create a Case Study for your chosen corporation/organization.              | • Give presentation in class  
                     • Submit written report                                                                 |