Course information:
Semester: Spring  
Course #: IS 257  
Year: 2013  
Title: Network Defense and Counter Measures  
CRN #: 28777  
Credits: 3

Instructor information:
Instructor: Joel Hutchins  
Cell Phone: Available in Courseroom (Leave message anytime if I am not available.)  
E-Mail: joel.hutchins@enmu.edu  
Office: NA - Course is online.  
Class Times: Online 24 x 7.

Rationale for student taking this course:
Provide students with the necessary understanding and abilities to apply tools, techniques and technologies used in the technical securing of information assets. This course prepares students to complete the Computer and Network Security Certification Program and other key security certifications. The course provides a basis for students to enter the computer and network security job market with the necessary knowledge to start being productive immediately.

Course description:
This course examines the tools, techniques and technologies used in the technical securing of information assets. Students will receive in-depth information about the software and hardware components of Information Security and Assurance.  
PREREQUISITE: IS 131

Text(s)/Study Guides(s), Manuals:
Guide to Network Defense and Countermeasures - Second Edition  
By: Weaver  

Required Material(s):

- ENMU E-mail Account  
- ENMU Ruidoso Blackboard Account  
- A Java capable desktop or laptop pc with Office software such as Open Office or Microsoft Office  
  – for viewing files
Expected student outcomes or competencies:
Upon successful completion of this course, the student should be able to:

Chapter 1
- Explain the fundamentals of TCP/IP networking
- Describe the threats to network security
- Explain the goals of network security
- Describe a layered approach to network defense
- Explain how network security defenses affect your organization.

Chapter 2
- Explain the fundamental concepts of risk analysis
- Describe different approaches to risk analysis
- Explain the process of risk analysis
- Describe techniques to minimize risk

Chapter 3
- Explain best practices in security policies
- Formulate a security policy and identify security policy categories
- Explain the importance of ongoing risk analysis and define incident-handling procedures

Chapter 4
- Describe the concepts of signature analysis
- Detect normal and suspicious traffic signatures
- Identify suspicious events
- Explain the Common Vulnerabilities and Exposures (CVE) standard

Chapter 5
- Explain basic VPN concepts
- Describe encapsulation in VPNs
- Describe encryption in VPNs
- Describe authentication in VPNs
- Summarize the advantages and disadvantages of VPNs

Chapter 6
- Explain design considerations for a VPN
- Describe options for VPN configuration
- Explain how to set up VPNs with firewalls
- Explain how to adjust packet-filtering rules for VPNs
- Describe guidelines for auditing VPNs and VPN policies

Chapter 7
- Identify the components of an intrusion detection system
- Explain the steps of intrusion detection
- Describe options for implementing intrusion detection systems
- Evaluate different types of IDS products

Chapter 8
- Configure an IDS and develop filter rules
• Develop a security incident response team for your organization
• Explain the six-step incident response process
• Describe how to respond to false alarms to reduce reoccurrences
• Explain options for dealing with legitimate security alerts

Chapter 9
• Explain what firewalls can and cannot do
• Describe common approaches to packet filtering
• Establish a set of rules and restrictions for a firewall
• Design common firewall configurations
• Compare hardware and software firewalls

Chapter 10
• Explain the goal of securing the network perimeter
• Describe factors in choosing a bastion host
• Explain how to supplement a firewall with a proxy server
• Set up Network Address Translation (NAT)
• Decide when to use user, session, or client authentication

Chapter 11
• Manage firewalls to improve security
• Describe the most important issues in managing firewalls
• Know how to install and configure Check Point NG
• Know how to install and configure Microsoft ISA Server 2000
• Know how to manage and configure Iptables for Linux

Chapter 12
• Strengthen network control by managing security events
• Improve analysis by auditing network security procedures
• Strengthen detection by managing an intrusion detection system
• Improve network defense by changing a defense in depth configuration
• Strengthen network performance by keeping pace with changing needs
• Increase your knowledge base by keeping on top of industry trends

Prerequisites for the course:

IS 131 or Instructor's permission.

Integration of critical skills:

In this course, students will demonstrate the following critical skills by:

Upon satisfactory completion of this course, the student will develop the following critical skills:

1) Using Current Technology with extensive use of firewall security fundamentals will develop and apply firewall use skills in various networked environments.
2) Writing skills will be developed through group discussion exercises, internet research assignments, and the use of presentation software.
3) Critical thinking skills will be developed through problem solving exercises in related network and computing areas of security.
4) Skills in group work will be developed during computer network operation and group discussions.
5) Public communication skills will be developed through group discussions.

Course Grading Policy:

EXAMS: (200 points)
There will be two exams a Mid-tern and a final exam. Each exam will have a value of 100 points (200 points total), covering the material taught in-class and assigned from the textbook. The final exam will be comprehensive, covering material from the entire course. Student have a one week window to complete an exam, the exam must be completed in the designated time-frame or receive a zero.

CHAPTER ASSESSMENTS: (1400 points)
There will be 14 Quiz Assessments, one for each chapter in the book and in the online chapter learning module. Each assessment is worth 100 points for a total of 1400 points.

Group Discussions: (140 points) 10 points for each discussion topic completed.
Final grades will be awarded based on the total points earned for the course, according to the following scale:

A=1468 – 1632 Points (90%)  
B = 1306 – 1467 Points (80%)  
C=1142 – 1305 Points (70%)  
D=979 – 1142 Points (60%)  
F= Below 978 Points

The textbook will be heavily used for this class. Students are expected to read the assigned sections and follow along in the book while completing the online learning modules. Students should expect to put in extra time in order to complete all assignments and projects.

Tentative Course Outline:

<table>
<thead>
<tr>
<th>Week/ Date</th>
<th>Material covered/assignments</th>
<th>Work due</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/14 – 01/19</td>
<td>Week 1 - Chapter 1 Network Defense Fundamentals</td>
<td>Quiz1</td>
<td>See expected student outcomes or competencies on pages 2 &amp; 3 of this syllabus.</td>
</tr>
<tr>
<td>01/20 – 01/26</td>
<td>Week 2 - Chapter 2 System Policy Design: Risk Analysis</td>
<td>Quiz2</td>
<td></td>
</tr>
<tr>
<td>01/27 – 02/02</td>
<td>Week 3- Chapter 3 Security Policy Implementation</td>
<td>Quiz3</td>
<td></td>
</tr>
<tr>
<td>02/03 – 02/09</td>
<td>Week 4 - Chapter 4 Network Traffic Signatures</td>
<td>Quiz4</td>
<td></td>
</tr>
<tr>
<td>02/10 – 02/16</td>
<td>Week 5 - Chapter 5 Virtual Private Network (VPN) Concepts</td>
<td>Quiz5</td>
<td></td>
</tr>
<tr>
<td>02/17 – 02/23</td>
<td>Week 6 - Chapter 6 VPN Implementation</td>
<td>Quiz6</td>
<td></td>
</tr>
<tr>
<td>02/24 – 03/02</td>
<td>Week 7 - Chapter 7 Intrusion Detection System Concepts</td>
<td>Quiz7</td>
<td></td>
</tr>
<tr>
<td>03/03 – 03/09</td>
<td>Week 8 - Mid-term Exam</td>
<td>Review 1 - 7</td>
<td></td>
</tr>
<tr>
<td>03/10 – 03/16</td>
<td>Week 9 – Spring Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>03/17 – 03/23</td>
<td>Week 10 - Chapter 8 Intrusion Detection: Incident Response</td>
<td>Quiz8</td>
<td></td>
</tr>
<tr>
<td>03/24 – 03/30</td>
<td>Week 11 - Chapter 9 Part 1 Choosing and Designing Firewalls</td>
<td>Quiz9</td>
<td></td>
</tr>
<tr>
<td>03/31 – 04/06</td>
<td>Week 12 - Chapter 9 Part 2 Choosing and Designing Firewalls</td>
<td>Quiz10</td>
<td></td>
</tr>
<tr>
<td>04/07 – 04/13</td>
<td>Week 13 - Chapter 10 Firewall Topology</td>
<td>Quiz11</td>
<td></td>
</tr>
<tr>
<td>04/14 – 04/20</td>
<td>Week 14 - Chapter 11 Part 1 Strengthening and Managing Firewalls</td>
<td>Quiz12</td>
<td></td>
</tr>
<tr>
<td>04/21 – 04/27</td>
<td>Week 15 - Chapter 11 Part 2 Strengthening and Managing</td>
<td>Quiz13</td>
<td></td>
</tr>
</tbody>
</table>
No Smoking on Campus – Effective June 15, 2007 the Dee Johnson Clean Indoor Air Act prohibits smoking at all workplaces and public facilities. In order to comply with the provisions of the law, smoking is banned inside, or within 30 feet of any entrance way.

Children in the Classroom Prohibited – Children are not allowed in the classroom. Students bringing children to class will be dismissed.

Academic Integrity and Standards of Behavior – For the complete guide to services available to students and the academic and non-academic rules and regulations governing ENMU-Ruidoso students please refer to the Student Handbook available at http://www.ruidoso.enmu.edu/docs/studenthnbk.pdf.

Instructors at ENMU-Ruidoso will not tolerate poor student behavior including plagiarism. Plagiarism is:

- Offering the work of another as one's own;
- Offering the work of another without acknowledgment or
- Failing to give credit for quotations or essentially identical expressions of material taken from books, encyclopedias, magazines, other reference works, term papers, reports or sources of any other individual.

Punishment is left up to the instructor and may range from a written warning to expulsion from the university.

Americans with Disabilities Act:

If you have physical or learning needs that require accommodation, contact your instructor or Juanita Garcia, Student Affairs Coordinator (257-2120) at the beginning of the semester. All efforts will be made to accommodate these needs or to provide equipment necessary to accomplish the requirements for this course. Discussions and documentation will be kept confidential.

Inclement Weather Closing Policy:

Students should always assume that classes are meeting as scheduled unless a campus closure notice is posted on the ENMU-Ruidoso website or announced on the radio or television. In the event of a closure
due to inclement weather or other emergency, faculty will attempt to notify students in advance of the class meeting. Refer to the website for the complete Inclement Weather Closing Policy and Procedure.

**Class Cancellation Policy:**
Class meetings may not be cancelled by the instructor. If the instructor is ill or unable to hold class for reasons beyond his or her control, a substitute instructor will hold class or students will be given the opportunity to make up missed class time through an alternative meeting time (agreeable to all students) or by completion of an outside assignment.
Student Agreement

I have reviewed and understand the entire content of this syllabus and agree to perform in accordance with the information contained therein.

______________________________________
(Student signature)

Date