Modesto Junior College  
Course Outline of Record  
CMPSC 281

I. **OVERVIEW**  
The following information will appear in the 2010 - 2011 catalog

**CMPSC 281 Advanced Networking & Security**  
3 Units  

*Prerequisite:* Satisfactory completion of CMPSC 264.

Technical study of security for networks. Includes assessing security risks, planning administrative access and user accounts, securing communication channels, securing file and print resources, secure access to remote users and offices, secure network access to Internet users, extending the network to partner organizations, designing a public key infrastructure, and developing a security plan. Hands-on computer assignments required.  

Field trips might be required.  
(A-F or P/NP - Student choice) Lecture /Lab  
Transfer: (CSU)

II. **LEARNING CONTEXT**  
Given the following learning context, the student who satisfactorily completes this course should be able to achieve the goals specified in Section III, Desired Learning:

A. **COURSE CONTENT**

1. **Required Content:**

   a. Assessing Security Risks  
      i. Planning network security  
      ii. Identifying risks to data and services  
      iii. Establishing security standards

   b. Operating System Security  
      i. Security features of directory services  
      ii. Authenticating user accounts  
      iii. Securing access to resources  
      iv. Encryption technologies  
      v. Public key infrastructure technology

   c. Planning Administrative Access and User Accounts  
      i. Administrative models  
      ii. Designing group strategies  
      iii. Local and Remote administrative access  
      iv. Account creation and policies
v. Delegation of authority

d. Securing Systems and Resources
   i. Planning physical security
   ii. Designing and deploying security configuration templates
   iii. File systems security
   iv. Auditing resource access
   v. Backup and restore procedures
   vi. Protecting against viruses

e. Securing Communication Channels
   i. Assessing network data visibility
   ii. Designing multi-layer security
   iii. Deploying network traffic security

f. Securing Access to heterogeneous environments
   i. Secure network access for multiplatform clients
   ii. Monitoring for security breaches
   iii. Security for dial-up and VPN connections
   iv. Defining private and public networks
   v. Securing connections using routers

g. Secure Network Access to the Internet
   i. Identifying potential risks
   ii. Using firewalls
   iii. Using secured subnets
   iv. Planning Internet usage policies
   v. Managing Internet access through proxy server and client-side configuration

h. Extending the Network to Partner Organizations
   i. Providing access
   ii. Securing applications
   iii. Structuring directory services to manage partner accounts
   iv. Authenticating partners from trusted networks

   i. Public Key Infrastructure
i. Using certificates
ii. Certificate Life Cycle
iii. Certification authority
iv. Mapping certificates to user accounts
v. Maintenance strategies

j. Developing a Security Plan
   i. Defining security requirements
   ii. Maintaining the security plan

2. **Required Lab Content:**
   
   a. Investigate Security Risks
      i. Planning network security
      ii. Identifying risks to data and services
      iii. Establishing security standards
   
   b. Manipulate Operating System Security
      i. Security features of directory services
      ii. Authenticating user accounts
      iii. Securing access to resources
      iv. Encryption technologies
      v. Public key infrastructure technology
   
   c. Editing Administrative Access and User Accounts
      i. Using Administrative models
      ii. Implementing group strategies
      iii. Manipulate Local and Remote administrative access
      iv. Account creation and policies
      v. Delegation of authority
   
   d. Illustrating Securing Systems and Resources
      i. Implementing physical security
      ii. Deploying security configuration templates
      iii. Using File systems security
iv. Auditing resource access  
v. Apply Backup and restore procedures  
vi. Using anti-virus applications  

e. Implementing Communication Channels Security  
i. Assessing network data visibility  
ii. Deploying multi-layer security  
iii. Deploying network traffic security  

f. Demonstrate Access to heterogeneous environments  
i. Secure network access for multiplatform clients  
ii. Monitoring for security breaches  
iii. Security for dial-up and VPN connections  
iv. Illustrating private and public networks  
v. Securing connections using routers  

g. Demonstrate Secure Network Access to the Internet  
i. Identifying potential risks  
ii. Using firewalls  
iii. Using secured subnets  
iv. Produce Internet usage policies  
v. Managing Internet access through proxy server and client-side configuration  

h. Solve Extension of the Network to Partner Organizations  
i. Providing access  
ii. Securing applications  
iii. Structuring directory services to manage partner accounts  
iv. Authenticating partners from trusted networks  

i. Investigate Public Key Infrastructure  
i. Using certificates  
ii. Certificate Life Cycle  
iii. Certification authority  
v. Mapping certificates to user accounts  
v. Maintenance strategies
j. Apply a Security Plan
   i. Implement security requirements
   ii. Maintaining the security plan

B. **ENROLLMENT RESTRICTIONS**

1. **Prerequisites**
   Satisfactory completion of CMPSC 264.

2. **Requisite Skills**
   *Before entering the course, the student will be able to:*
   
   a. Explain networking concepts and skills
   b. Demonstrate an operating systems background including basic installation, configuring, and maintenance of client and server systems.

C. **HOURS AND UNITS**

<table>
<thead>
<tr>
<th>INST METHOD</th>
<th>TERM HOURS</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lect</td>
<td>36</td>
<td>2.00</td>
</tr>
<tr>
<td>Lab</td>
<td>54</td>
<td>1.00</td>
</tr>
<tr>
<td>Disc</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

D. **METHODS OF INSTRUCTION (TYPICAL)**

*Instructors of the course might conduct the course using the following method:*

1. Lecture and Discussion Methods
2. Classroom Demonstrations
3. Technology Presentations
4. Question and Answer Sessions
5. Lab Demonstrations
6. Practical Hands-On Exercises
7. Independent Study through readings

E. **ASSIGNMENTS (TYPICAL)**

1. **EVIDENCE OF APPROPRIATE WORKLOAD FOR COURSE UNITS**
   *Time spent on coursework in addition to hours of instruction (lecture hours)*

   a. *(Weekly)* Write one-page summaries of security articles published in leading telecommunications journals, by standards organizations, and texts.

   b. *(Weekly)* Carefully analyze and follow detailed instructions for completion of projects.
c. (Weekly) Quizzing on security concepts and terminology.

d. (Weekly) Lab activities focused on hands-on implementation of network security concepts and solutions.

e. (Per term) Compare and contrast different network security systems, security hardware, and security software components as well as security computer codes.

f. (Per term) Design solution algorithms for network security problems and implement those solutions using systems analysis techniques and telecommunications programs.

g. (Per term) Several exams at strategic points during the term.

2. **EVIDENCE OF CRITICAL THINKING**

   *Assignments require the appropriate level of critical thinking*

   a. Assignment: A local community college has contracted with Northridge Security Consultants (NSC) to help them investigate automated patch update services. NSC has asked you to help them with this project.

      i. Create a PowerPoint presentation of 6-8 slides about automated patch update services. Include how they differ from desktop updates (using the vendor’s online update service memo), their advantages, their disadvantages, the additional hardware and software necessary, and projected costs.

      ii. The community college appreciated your presentation but has decided to not invest in an automated patch update service. NSC is concerned that this may weaken their security on campus and has asked you to write a memo to the Security Director explaining why they are preferred in an organizational setting over desktop updates. Add to your memo three scenarios of how desktop updates could make the organization more vulnerable.

   b. Lab Project: In this project, you download and install Microsoft’s RootkitRevealer tool to help detect the presence of a rootkit.

      i. Open your Web browser and enter the URL [www.microsoft.com/technet/sysinternals/Security/RootkitRevealer.mspx](http://www.microsoft.com/technet/sysinternals/Security/RootkitRevealer.mspx). The location of content on the Internet such as this program may change without warning. If you are no longer able to access the program through the above URL, then use a search engine like Google ([www.google.com](http://www.google.com)) and search for “RootkitRevealer”.

      ii. Scroll to the bottom of the page and click on Download RootkitRevealer (231 KB). When the File Download dialog box appears, click Save and download the file to your desktop or another location designated by your instructor.

      iii. When the download is complete, click Open to open the compressed (.ZIP) file. If you receive a warning that a Web site wants to open Web content using the program, click Allow.

      iv. Click Extract all files to launch the Extraction Wizard. Follow the steps in the wizard to extract all files to your desktop or another location designated by your instructor.

      v. Navigate to the location where the files were extracted and start the program by double-clicking on RootkitRevealer.exe. If you receive an Open File—Security Warning dialog box click Run. Click Agree to the RootkitRevealer License Agreements.

      vi. The RootkitRevealer screen will appear.

      vii. Click File and then Scan to begin a scan of the computer for a rootkit.
c. Example Quiz/Exam Questions:
   i. A(n) ____________________ attack attempts to consume network resources so that the network or its devices cannot respond to legitimate requests.
   ii. The split between the network and host portions of the IP address originally was set on the boundaries between the bytes (called ____________________).
   iii. Because of the weaknesses of WEP it is possible for an attacker to identify two packets derived from the same IV (called a(n) ____________________).
   iv. The most common logical access control is a(n) ____________________, sometimes referred to as a logical token.
   v. What are the methods used by NAC to direct the client to a quarantine VLAN

F. TEXTS AND OTHER READINGS (TYPICAL)


III. DESIRED LEARNING

A. COURSE GOAL
As a result of satisfactory completion of this course, the student should be prepared to:

   analyze security over networks, system security within networks, and security business requirements;
   evaluate network security architecture; and construct authentic network security strategies.

B. STUDENT LEARNING GOALS
Mastery of the following learning goals will enable the student to achieve the overall course goal.

1. Required Learning Goals
Upon satisfactory completion of this course, the student will be able to:

   a. Analyze business requirements for security.
   b. Analyze physical and information system security within a network.
   c. Analyze technical requirements for networking.
   d. Design network security architecture.
   e. Analyze network security requirements.
   f. Design a network security plan.
   g. Design an authentication strategy for the network.
   h. Implement Public Key infrastructure components.
   i. Design a VPN strategy for network security.
   j. Implement a VPN in a network environment.
   k. Analyze security over the Internet.
   l. Troubleshoot network security.
2. **Lab Learning Goals**

Upon satisfactory completion of the lab portion of this course, the student will be able to:

a. Apply business requirements for security.

b. Diagram physical and information system security within a network.

c. Illustrate technical requirements for networking with appropriate technology.

d. Produce network security architecture in a lab setting.

e. Investigate network security requirements through hardware network devices and software management tools.

f. Implement a network security plan for a defined lab network.

g. Utilize an authentication strategy for a computer network.

h. Diagram and apply Public Key infrastructure components.

i. Describe and use a VPN in a controlled network environment.

j. Investigate Internet security through appropriate network security software tools.

k. Troubleshoot network security protocols utilizing appropriate technology.

IV. **METHODS OF ASSESSMENT (TYPICAL)**

A. **FORMATIVE ASSESSMENT**

1. Assignments

2. Quizzes

3. Lab Activities

4. Exams

B. **SUMMATIVE ASSESSMENT**

1. Assignments

2. Quizzes

3. Lab Activities

4. Exams