

PALOMAR COLLEGE
COURSE OUTLINE OF RECORD FOR
DEGREE CREDIT COURSE

X Transfer Course X A.A. Degree applicable course
(check all that apply)

COURSE NUMBER AND TITLE: CSIS 168 Designing Network Security

UNIT VALUE: 2

MINIMUM NUMBER OF SEMESTER HOURS: 40

BASIC SKILLS REQUIREMENTS: Appropriate language and computational skills.

ENTRANCE REQUIREMENTS

PREREQUISITE: None

COREQUISITE: None

RECOMMENDED PREPARATION: CSIS 165

SCOPE OF COURSE:

This course provides students with the knowledge and skills necessary to design a security framework for small, medium, and enterprise networks using Microsoft Windows technologies.

SPECIFIC COURSE OBJECTIVES:

Analyzing Business Requirements
Analyzing Technical Requirements
Analyzing Security Requirements
Designing a Windows 2000 Security Solution
Designing a Security Solution for Access Between Networks
Designing Security for Communication Channels

CONTENT IN TERMS OF SPECIFIC BODY OF KNOWLEDGE:

- I. **Assessing Security Risks**
 - A. Identifying Risks to Data
 - B. Identifying Risks to Services
 - C. Identifying Potential Threats
 - D. Introducing Common Security Standards
 - E. Planning Network Security
- II. **Introducing Windows Security**
 - A. Introducing Security Features in Active Directory

- B. Authenticating User Accounts
- C. Securing Access to Resources
- D. Introducing Encryption Technologies
- E. Encrypting Stored and Transmitted Data
- F. Introducing Public Key Infrastructure Technology
- III. **Providing Secure Access to Local Network Users**
 - A. **Planning Administrative Access**
 - B. Determining the Appropriate Administrative Model
 - C. Designing Administrative Group Strategies
 - D. Planning Local Administrative Access
 - E. Planning Remote Administrative Access
- IV. **Planning User Accounts**
 - A. Designing Account Policies and Group Policy
 - B. Planning Account Creation and Location
 - C. Planning Delegation of Authority
 - D. Auditing User Account Actions
- V. **Securing Windows–Based Computers**
 - A. Planning Physical Security for Windows–based Computers
 - B. Evaluating Security Requirements
 - C. Designing Security Configuration Templates
 - D. Evaluating Security Configuration
 - E. Deploying Security Configuration Templates
- VI. **Securing File and Print Resources**
 - A. Examining Windows File System Security
 - B. Protecting Resources Using DACLs
 - C. Encrypting Data Using EFS
 - D. Auditing Resource Access
 - E. Securing Backup and Restore Procedures
 - F. Protecting Data from Viruses
- VII. **Securing Communication Channels**
 - A. Assessing Network Data Visibility Risks
 - B. Designing Application-Layer Security
 - C. Designing IP-Layer Security
 - D. Deploying Network Traffic Encryption
- VIII. **Providing Secure Access to Non-Microsoft Clients**
 - A. Providing Secure Network Access to UNIX Clients
 - B. Providing Secure Network Access to NetWare Clients
 - C. Providing Secure Access to Macintosh Clients
 - D. Securing Network Services in a Heterogeneous Network
 - E. Monitoring for Security Breaches
 - F. **Providing Secure Access to Remote Users and Offices**
- IX. **Providing Secure Access to Remote Users**
 - A. Identifying the Risks of Providing Remote Access
 - B. Designing Security for Dial-Up Connections
 - C. Designing Security for VPN Connections
 - D. Centralizing Remote Access Security Settings
- X. **Providing Secure Access to Remote Offices**
 - A. Defining Private and Public Networks
 - B. Securing Connections Using Routers
 - C. Securing VPN Connections Between Remote Offices
 - D. Identifying Security Requirements

- E. **Providing Secure Access Between Private and Public Networks**
- XI. **Providing Secure Network Access to Internet Users**
- XII. **Providing Secure Internet Access to Network Users**
 - A. Protecting Internal Network Resources
 - B. Planning Internet Usage Policies
 - C. Managing Internet Access Through Proxy Server Configuration
 - D. Managing Internet Access Through Client-Side Configuration
- XIII. **Providing Secure Access to Partners**
- XIV. **Extending the Network to Partner Organizations**
 - A. Providing Access to Partner Organizations
 - B. Securing Applications Used by Partners
 - C. Securing Connections Used by Remote Partners
 - D. Structuring Active Directory to Manage Partner Accounts
 - E. Authenticating Partners from Trusted Domains
- XV. **Designing a Public Key Infrastructure**
 - A. Introducing a Public Key Infrastructure
 - B. Using Certificates
 - C. Examining the Certificate Life Cycle
 - D. Choosing a Certification Authority
 - E. Planning a Certification Authority Hierarchy
 - F. Mapping Certificates to User Accounts
 - G. Managing CA Maintenance Strategies
- XVI. **Developing a Security Plan**
 - A. Designing a Security Plan
 - B. Defining Security Requirements
 - C. Maintaining the Security Plan

REQUIRED READING: Microsoft Official Curriculum – Designing a Secure Microsoft Windows Network

SUGGESTED READING: None

REQUIRED WRITING:

Problem solving exercises and skills demonstrated in computer homework assignments. A minimum of one page per homework assignment is required.

OUTSIDE ASSIGNMENTS:

Students are expected to spend a minimum of three hours a week practicing the skills learned in class on their home machines. The midterm and final are both take home exams requiring at least 10 hours to complete.

INSTRUCTIONAL METHODOLOGY:

Check all that apply:

- lecture
- laboratory
- lecture-laboratory combination
- directed study

DISTANCE LEARNING:

This course may be offered as a distance learning course and meets Title 5 regulations 55370, 55372, 55374, 55376, 55378, and 55380.

Yes No

If yes, check all that apply:

- Television Course (Video one-way, e.g. ITV, video cassette, etc.)
- Online Course (Text one-way, e.g. newspaper, correspondence, electronic file, etc.)
- Two-Way Video Conferencing (Two-way interactive video and audio)
- One-Way Video Conferencing (One-way interactive video and two-way interactive audio)
- Computer Assisted Instruction (A specialized form of mediated instruction relying primarily on student access to information and prepared lessons or teaching materials through a computer terminal, but not under immediate supervision of a qualified instructor.)

GRADING POLICY AND STANDARDS (include methods of determining whether the stated objectives have been met by students):

Grades for courses are based upon final examinations, mid-term examinations, other tests, assignments, projects, and participation. Faculty will inform students of their grading policy at the beginning of each semester.

IS COURSE REPEATABLE FOR REASON(S) OTHER THAN DEFICIENT GRADE?

Yes No Number of times course may be taken for credit:

If yes, identify specific provision of Title 5 Division 2 section(s), 55761-55763 and 58161 which qualifies course as repeatable:

CONTACT PERSON: Terrie Smith x2610

SIGNATURES:

SIGNATURES ON FILE
