Computer Science Department
cs.salemstate.edu

ITE 410 Network Design and Security 4 cr.

Catalog description:

This course offers an in-depth look at the top-down design of networks, taking into consideration the business requirements and goals, and understanding the methodologies and techniques employed in designing a complex campus-level and enterprise-level network infrastructure. Topics include: identifying customer needs and goals, logical and physical network design, designing models for addressing and numbering, selecting switching and routing protocols, developing network security strategies, and selecting technologies and devices for campus and enterprise networks. Four lecture hours per week.

Prerequisites: ITE 315

Course Narrative:

This course is on in-depth understanding of designing computer networks, taking into consideration the security measures. Students already familiar with fundamentals of computer and network architectures and the nature of security threats that exists in the globally connected environment will be able to learn "how to design." That is, they will be able to design a network for a campus and enterprise top down. IT professionals who know how to design a network can resolve any issues that can potentially impact the smooth working of a network infrastructure. They can easily administer, test, and optimize the network performance.

This course begins with identifying and analyzing the business goals and constraints, technical goals, and tradeoffs. After ensuring the needs of an infrastructure, logical network design is put together that includes designing network topology, models for addressing and numbering, selecting switching and routing protocols, taking into consideration the security measures for securing networks and hence developing network security strategies, and developing network management strategies. Once the logical aspect of network design is complete, the physical aspect of network design will be taken into consideration where selecting the technologies and devices for campus and enterprise networks are considered. Testing, optimizing and documenting forms the last component of a network design.

Goals:

G1: This course will enable students to clearly analyze the goals and requirements of an enterprise in terms of network design and deployment;

G2: This course will demonstrate the knowledge of issues in network design and security and in-depth understanding of techniques, tools, and mechanisms used to provide solutions;

G3: This course will enable students to apply the knowledge of network design and security in actually designing the network for an IT enterprise.

G4: This course will demonstrate the understanding and skill required for testing and vulnerability assessment and documenting the network design.

Course Objectives:

Upon successful completion of the course, a student will have demonstrated the ability to:

O1: apply correct technical terminology when analyzing requirements, describing the main issues, and offering solutions for building secure IT infrastructures;

O2: use in-depth knowledge of protocols, algorithms, mechanisms, and tools used in designing and construction of IT network infrastructure and apply these techniques in practice;

O3: apply assessment techniques and use tools that allow IT managers to test and asses vulnerabilities of their infrastructures;

O4: analyze results of testing and vulnerability assessment, document, and design solutions to deploy networks.

Course Objective / Assessment Mechanism matrix

Program Objective (condensed form)	**CO01**	**CO02**	**CO03**	**CO04**
PO-01: Knowledge of and ability to use terminology, concepts, and technology employed in the design, construction, and use of IT infrastructures	✓	✓	✓	✓
PO-02: Understanding of best practices and standards used in the IT field and their application to problem solving	✓	✓		
PO-03: The ability to understand implementation of an IT infrastructure, analyze a situation, and to communicate to IT professionals	✓	✓	✓	✓
PO-04: The ability to identify computing technologies and integrate them into solutions, including integration into the end-user environment	✓	✓		
PO-05: The ability to present an analysis of a problem and possible solutions, to perform risk assessment, to generate documentation, and to test and verify a solution	✓	✓	✓	✓
PO-06: The ability to communicate effectively and work cooperatively with stakeholders, users, and fellow IT professionals	✓	✓	✓	✓
PO-07: The ability to identify and analyze stakeholder and user needs and take them into account in the selection, creation, evaluation and administration of an IT environment	✓	✓		
PO-08: An awareness of the human, ethical, legal, and societal issues relating to the impact of IT on all facets of society				
PO-09: Recognition of the need for and an ability to engage in continuing professional development				

Course topics:

- Identifying Customer's Needs and Goals IAS1(1), NET1(1)
    - Analyzing Business Goals and Constraints
    - Analyzing Technical Goals and Tradeoffs
    - Characterizing the Existing Internetwork
    - Characterizing Network Traffic
- Logical Network Design IAS6(1), NET4(2), PT2(1)
    - Designing a Network Topology
    - Designing Models for Addressing and Numbering
    - Selecting Switching and Routing Protocols
    - Developing Network Security Strategies
    - Developing Network Management Strategies

- Physical Network Design
    - Selecting Technologies and Devices for Campus Networks
    - Selecting Technologies and Devices for Enterprise Networks IAS1(2)
- Testing Optimizing and Documenting Your Network Design PT1(1), PT3(1)
    - Testing Your Network Design
    - Optimizing Your Network Design
    - Documenting Your Network Design

NET1(2)

- Security threats to an IT infrastructure IAS3(3), IAS5(3), IAS10(1), IAS11(1), NET4(1), SA3(2)
- Security countermeasures in IP networks IAS9(1), IAS10(1), IAS11(1), NET4(2), NET5(1)
- Security of IT infrastructures IAS2(2), IAS4(3), IAS7(1), IAS9(2), NET5(2)
- Data storage security IM3(1), NET6(3)
- Security in WWW WS2(1), WS5(2)

Organization of the course

The course consists of lectures, labs, homework assignments, quizzes, and two exams – a midterm and a final. Lectures include exercises that may consist of:

- Discussions of the material presented during lectures
- Analysis of IP network and its security problems and solutions
- Analysis of IP infrastructure security threats and writing of reports that offer solutions used to mitigate these threats
- Usage of tools available to IT professionals to analyze networks and examine security threats

Group discussion time and group presentations that will be conducted as part of the scheduled laboratory sessions are an integral component of the course, serving to reinforce the concepts and techniques presented during lectures. Specific requirements for each assignment will be stated when the assignment is distributed; all written submissions will be graded against the Writing rubric. Presentations will be assessed based on the Presentation rubric.

Assignments:

Homework assignments include analysis of network components and design of solutions for network and security-related tasks, as well as exercises in using network and security tools. Assignments require students to use information given during the lectures and textbooks, and perform Internet research for necessary materials. Regular writing assignments include but are not limited to:

- review of technical articles;
- presentation of research findings;
- proposals to solve different security problems formulated by the instructor;
- analysis and evaluation of methodologies used in building secure networked environments;

Labs:

Weekly labs consist of hands-on exercises that include:

- Analyzing different network and security architectures and writing reports
- Running testing and vulnerability assessment tools
- Analyzing different distributed environments from a security point of view and suggesting changes to improve security

Some of labs will be combined into projects. All lab/project reports must conform to guidelines announced in class. Projects will be assessed and graded against the Project Implementation rubric.

Quizzes, Tests and Examinations: There will be four quizzes (each covering a major topic), a midterm, and a cumulative final. Quizzes and exams will include multiple choice and problem solving tasks.

Grading: Final grades will be determined on the basis of the following approximate weights:

• Laboratory exercises	20%
• Homework assignments	25%
• Quizzes	25%
• Midterm exam	15%
• Final exam	15%

Course Objective / Assessment Mechanism matrix

	Lab assignment	Homework assignment	Quizzes	Midterm exam	Final Exam
CO1	✓	✓	✓	✓	✓
CO2	✓	✓	✓	✓	✓
CO3	✓	✓			
CO4	✓	✓			

Textbook

M. Chiampa. Security+ Guide to network security fundamentals. Fourth Edition. Cengage Learning, 2011

Bibliography:

J. F. Kurose, K.W. Ross. Computer networking. Fifth Edition. Addison-Wesley, 2010.
W. Stallings, L. Brown. Computer security. Second Edition. Pearson Education, 2012.
M. Whitman et al. Guide to firewalls and network security. Second Edition. Cengage Learning, 2009.
S. A. Thomas. IPng and the TCP/IP protocols. First Edition. Wiley, 1996.
H. X. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001.
S. Chouldhury. Public Key Infrastructure: Implementation and Design. M&T books, 2002.
A. Basta, W. Halton. Computer security and penetration testing. Thomson Course Technology, 2008.
M. Simpson. Hands-on Ethical hacking and network defense. Thomson Course Technology, 2006.
A. Basta, M. Zgola. Database security. First Edition. Cengage Learning, 2011.