Las Positas CurricUNET

LAS POSITAS COLLEGE

Las Positas College
3000 Campus Hill Drive
Livermore, CA 94551-7650
(925) 424-1000
(925) 443-0742 (Fax)

Course Outline for CNT 69

NETWORK SECURITY SEC+

Effective: Fall 2006

I. CATALOG DESCRIPTION:
CNT 69 — NETWORK SECURITY SEC+ — 3.00 units

Following the Sec+ certification objectives, an introduction to the concepts and practices of secure network design and management using desktop and network operating systems, router and switch operating systems, hardware and software Firewall and VPN technology for wired and wireless systems. The program will include authentication methods and devices, protocol analysis and IP network troubleshooting, strategies for identifying and countering vulnerabilities, network medias and topologies in a secure network, intrusion detection and forensic incident response.

2.50 Units Lecture 0.50 Units Lab

Strongly Recommended
CNT 62B - Cisco Networking Academy CCNA II

-

Grading Methods:
Letter or P/NP

Discipline:

	MIN
Lecture Hours:	45.00
Lab Hours:	27.00
Total Hours:	72.00

II. NUMBER OF TIMES COURSE MAY BE TAKEN FOR CREDIT: 2

III. PREREQUISITE AND/OR ADVISORY SKILLS:

Before entering this course, it is strongly recommended that the student should be able to:

A. CNT62B

IV. MEASURABLE OBJECTIVES:

Upon completion of this course, the student should be able to:

1. demonstrate an understanding of basic network security concepts;
2. create a secure network design using methods of authentication;
3. describe and evaluate methods of countering denial-of-service attacks;
4. discuss the methods and techniques of secure remote access;
5. describe how to protect email using PGP and S/MIME;
6. use protocol analyzer software to record and analyze network traffic;
7. demonstrate an understanding of web-based exploits and malware;
8. discuss how to utilize directory services like LDAP;
9. demonstrate an understanding of secure network media types;
10. demonstrate the ability to configure Network Address translation;
11. discuss and evaluate operating system vulnerabilities and OS hardening practices;
12. demonstrate an understanding of modern cryptography concepts as they relate to network security, such as steganography and PKI certificates;
13. discuss the characteristics of a physically secure network design;
14. describe and evaluate procedures for and the importance of disaster recovery and incident response planning.

V. CONTENT:

A. Network Security terminology, purpose and goals
   1. CompTIA Sec+ Exam
   2. Security careers
   3. Terminology
   4. Security goals

B. Objectives for Sec+
   1. Knowledge domains

        2. Test objectives
    C. Web security
        1. Internet vulnerabilities
        2. Best practices
        3. Secure web traffic
        4. Email and web server systems
        5. Troubleshooting methods, tools, skills
    D. Directory and enterprise services
        1. Active directory
        2. PKI
    E. Network fundamentals
        1. OSI model for Sec+
        2. TCP/IP for Sec+
        3. IP addressing for Sec+
        4. Network devices and concepts
        5. Troubleshooting methods, tools, skills
    F. Routers switches & servers in a secure network
        1. Routing protocols for Sec+
        2. Switch fabric
        3. Secure networks
        4. Network policy
        5. Troubleshooting methods, tools, skills
    G. Firewalls & VPN
        1. ACLs
        2. Firewall design
        3. Remote users
        4. VPN
        5. Access policy
        6. Troubleshooting methods, tools, skills
    H. NAT and DMZs
        1. NAT / PAT
        2. Enterprise services planning
        3. DMZs
        4. Troubleshooting methods, tools, skills
    I. Cryptography and Steganography
        1. Data hiding
        2. Image encryption
        3. Email crime
        4. Passwords
    J. OS Hardening / Whitehat hacking / IDS
        1. Attacker profiles
        2. Attack types
        3. DoS, Malware, MiM
        4. Physical security
        5. Baselining
        6. Best practices
        7. IDS / Whitehat
        8. Methods, tools, skills
    K. Disaster Planning / Business continuity / Forensics
        1. Identity management
        2. Change / digital rights management
        3. Incident policy, Security policy
        4. Training and education
        5. Forensic investigation
        6. Methods, tools, skills

VI. METHODS OF INSTRUCTION:
    A. **Lecture** -
    B. **Demonstration** -
    C. **Research** -
    D. **Lab** -
    E. Assigned reading
    F. **Discussion** -

VII. TYPICAL ASSIGNMENTS:

A. Reading / listening to presentations and readings 1. Presentations and lectures Example: Lecture on VPN/IPSec 2. Selected current online readings Example: read Cisco Secure Desktop tutorial, at www.cisco.com B. Search for relevant material and read 1. Students use search engines to find readings relevant for each module. Example: Find resources describing Man in the Middle attacks, select 3 to read C. Provide comments regarding curriculum 1. Discussion and response questions accompany each module. Example: “Discuss how ARP cache poisoning threatens web servers.” D. Answer comments and questions from fellow students and instructor 1. Students must participate in group discussion Example: On the Cisco.com website, examine and discuss the history of PIX IOS vulnerabilities.

VIII. EVALUATION:
    A. **Methods**

    B. **Frequency**

        1. Frequency
            a. 6-10 module assignments
            b. Weekly discussion of group work
            c. 6-10 module quizzes
            d. 6-10 labs
            e. 1 final project
        2. Typical quiz question
            a. What is the difference between FAT32 and FAT16?
            b. Describe the difference between PING and TRACEROUTE
        3. Final exam

IX. TYPICAL TEXTS:

1. Mark Ciampa, Enfinger, Stuart *, Security + Guide to Networking Security Fundamentals.*, Course Technology, 2004.
2. Paul Cretaro *Lab Manual for Security +, .*, Course Technology, 2004.

X. OTHER MATERIALS REQUIRED OF STUDENTS:

A. Students require access to a computer connected to the Internet, with word processing and browser software, and an email address.