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; COMPTIA SECURITY + CERTIFICATION

Effective: Spring 2019

I. CATALOG DESCRIPTION:
CNT 69 — NETWORK SECURITY; COMPTIA SECURITY + CERTIFICATION — 3.00 units

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability. This course provides 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 includes authentication methods and devices, protocol analysis and IP network troubleshooting, strategies for identifying and countering vulnerabilities, network media and topologies in a secure network, intrusion detection and forensic incident response. CompTIA Security+ meets the ISO 17024 standard and is approved by U.S. Department of Defense. Security+ is also compliant with government regulations under the Federal Information Security Management Act (FISMA).

2.50 Units Lecture 0.50 Units Lab

Strongly Recommended
CNT 51 - CompTIA's A+ Certification Computer Technician
with a minimum grade of C

CNT 52 - Networking Fundamentals
with a minimum grade of C

Grading Methods:
Letter or P/NP

Discipline:
- Computer Service Technology

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

II. NUMBER OF TIMES COURSE MAY BE TAKEN FOR CREDIT: 1

III. PREREQUISITE AND/OR ADVISORY SKILLS:

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

A. CNT51
1. Build a personal computer, according to customer requirements
2. Install, configure, and maintain devices, and PCs for end users
3. Install and configure networking adapters, including the connectivity software
4. Install, update, and configure the Windows OS
5. Troubleshoot and document common hardware problems
6. Deploy desktop imaging, and install a virtual machine on a computer, using different hypervisors
7. Identify and explain system boards components, types and features
8. Select the correct memory types for specific expansion slots
9. Install and configure peripherals, input devices and printers
10. Secure a computer using anti-malware software and user access rights
11. Harden a wireless access point security and train end user in basic security features
12. Practice the appropriate communication skills and professionalism needed to provide effective customer support

B. CNT52
1. list and explain the layers of the OSI model and the TCP/IP Stack and desribe the roles of protocol layers in data networks;
2. describe and differentiate the devices, protocols, and services used to support communications in data networks and the Internet;
3. build a router and switch topology; and configure the devices to communicate with computers;
4. compose CISCO command-line interface (CLI) commands to perform basic router and switch configration;

    5. identify the responsibilities of a LAN system administrator;
    6. draw typical network diagrams, using software tools such as Microsoft Visio;
    7. monitor the network activity using monitoring tools to view packets and analyze traffic.

IV. MEASURABLE OBJECTIVES:

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

A. Discuss basic network security concepts
B. Create a secure network design using methods of authentication
C. Describe and evaluate methods of countering denial-of-service attacks
D. Discuss the methods and techniques of secure remote access
E. Describe how to protect email using PGP and S/MIME
F. Use protocol analyzer software to record and analyze network traffic
G. Explain web-based exploits and malware
H. Discuss how to utilize directory services like LDAP
I. Identify secure network media types
J. Configure Network Address translation
K. Discuss and evaluate operating system vulnerabilities and OS hardening practices
    1. Explain modern cryptography concepts as they relate to network security, such as steganography and PKI certificates
L. Discuss the characteristics of a physically secure network design
M. 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. Access 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. Online flash based training
   Example: Complete Skillsoft training module for CompTIA Sec+ on PKI configuration

D. Write reports
   Example: analyze an example network for security flaws, describe, and provide mitigation strategies

VIII. EVALUATION:

Methods/Frequency

A. Exams/Tests
   Final project, once
B. Quizzes
   Weekly
C. Group Projects
   Weekly
D. Class Participation
   Online or in person discussions weekly
E. Lab Activities
   Weekly

IX. TYPICAL TEXTS:

1. Ciampa , Mark *Security+ Guide to Network Security.* 4 ed., Cengage Press, 2011.
2. Brotherston, Lee . *Defensive Security Handbook: Best Practices for Securing Infrastructure.* 1 ed., O'Reilly Media, 2017.
3. Meyers, Mike. *Mike Meyers' CompTIA Security+ Certification Guide, Second Edition (Exam SY0-501).* 2nd Edtion ed., McGraw-Hill Education, 2017.
4. Christy, S. Russell, and Chuck Easttom. *CompTIA Security+ Practice Tests: Exam SY0-501.* first ed., Sybex, 2018.
5. Association of Computing Machinery ACM.org student membership

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
B. Association of Computing Machinery ACM.org student membership