Department Master Syllabus
Camden County College
Blackwood, New Jersey

Course Title: Linux Networking and Security

Course Number: CIS-285

Department/Program Affiliation: Computer Information Systems

Date of Last Revision: **April, 2018**
(This Department Master Syllabus has been examined by the program/department faculty members and it is decided a change requiring a revision is necessary at this time.)

Credits: 3

Contact Hours: 3 **Lecture 3** **Lab** 0 **Other** 0

Prerequisites: CIS–181, CSC-171, CST-102

Co-requisites: None

Course Description: This course is designed to give the student a working knowledge of Administration of the Linux/UNIX operating system in a security context. This includes the TCP/IP protocol, configurations and use of network access and data and system protection in the Linux and UNIX system. The student will learn to create Ethernet configurations in Linux and UNIX systems from a data security perspective and to configure network start ups, and services such as Telnet, FTP, and NFS as well as to use access control to develop effective firewalls and deny malicious agents in a host and to develop a mostly closed policy. Domain Name Server services will be learned as well as zoning, and secondary DNS. This course is taught in a room with computers for the explicit teaching of a computer skill set using lecture. Computers are used as a lecture tool to provide demonstrations and illustrations of the technical concepts taught. Access to computers provides the students with the advantage of interacting with the concepts presented. No graded assignments or mandatory exercises are completed during the lecture. Hands-on assignments are completed outside of class.

Course Student Learning Outcomes: Cognitive, Psychomotor, Affective Domains)

1. Outline the major components of the TCP/IP services in a Linux/UNIX Operating System as assessed through hands-on projects, exercises and tests by which the student shows comprehension of the major components of the TCP/IP Protocol in Linux/UNIX Operating System.
2. Describe the binary numbering system for IP Address access, network, broadcast, subnets, and configuring subnet masks as assessed through hands-on projects in which the students, creates networks setting broadcast and subnets and using subnet mask upon established rubrics.
3. Configure Ethernet access on a Linux system as assessed through hands-on projects, exercises and tests in which the student creates and diagrams a Linux/UNIX Ethernet port and services.

4. Create network services using telnet, xinetd, wu-ftpd, and inetd as assessed through hands-on projects, exercises and tests in which the student creates and diagrams a Linux/UNIX Ethernet port and services
5. Use access controls to deny a host/user and to develop a mostly closed security policy as assessed through hands-on projects, exercises and tests in which the student describes, creates, and manages access controls from other internet service access.
6. Describe, create, and manage a domain name server as assessed through hands-on projects, exercises and tests in which the student demonstrates the purpose and configuration of a domain name server (DNS).
7. Install and configure a secure web server using learned network and data security techniques described throughout the class.
8. Demonstrate the purpose and setup of secondary domain name servers as assessed through hands-on projects, exercises and tests in which the student demonstrates the purpose and configuration of a secondary DNS..
9. Explain binding and zone files through hands-on projects, exercises and tests in which the student explains the use of the bind function and zone files.
10. Build a secure filesharing network that relies on the security concepts discussed throughout the course, including firewalls and data encryption.
11. Build a model network "demilitarized zone" designed to protect the network from malicious agents using firewalls and other TCP/IP concepts.

Course Outline:

1. Course overview
2. Runlevels and Daemons
3. Booting Linux securely
4. Using the Vi editor
5. Filesystems and sharing
6. Data and system Integrity
7. Disk Quotas
8. File and Folder Permissions and Ownership
9. MAC Administration using SELinux, PAM and AppArmor
10. Firewall Concepts using IPTables and TCPWrapper
11. Host Security
12. Security Administration Concepts
13. Data Encryption

Course Activities: The classroom activities will include formal and informal lectures where new material and assigned problems will be explained. Students will have the opportunity to contribute to the discussion and to ask questions about the material. "Hands-on" work on the computer will be done outside of regularly scheduled classroom hours.

Assessment of Student Learning Outcomes: The student will be evaluated on the degree to which the above student learning outcomes are achieved. A variety of methods may be used such as tests, class participation, projects, homework assignments, etc.

1. Assessment through hands-on projects, exercises and tests in which the student shows comprehension of the major components of the TCP/IP Protocol in Linux/UNIX Operating System.

2. Assessment through hands-on projects in which the students, creates networks setting broadcast and subnets and using subnet mask upon established rubrics.
3. Assessment through hands-on projects, exercises and tests in which the student creates and diagrams a Linux/UNIX Ethernet port and services.
4. Use and test access controls to deny a host/user and to develop a mostly closed security policy as assessed through hands-on projects, exercises and tests in which the student describes, creates, and manages access controls from other internet service access.
5. Assessment through hands-on projects, exercises and tests in which the student describes, creates, and manages access controls from other internet service access.
6. Assessment through hands-on projects, exercises and tests in which the student demonstrates the purpose and configuration of a domain name server (DNS).
7. Build and test a secure filesharing network that relies on the security concepts discussed throughout the course, including firewalls and data encryption.
8. Assessment through hands-on projects, exercises and tests in which the student demonstrates the purpose and configuration of a secondary DNS
9. Build and test a model network "demilitarized zone" designed to protect the network from malicious agents using firewalls and other TCP/IP concepts.

Course Materials:
Textbook(s): Text: Course textbook: *Security Strategies in Linux Platforms and Applications*, 2nd ed.
Author: Jang, Michael and Ric Messier.
Publisher: Jones & Bartlett Burlington, MA:, 2017
ISBN-13: 978-1284031652
ISBN-10: 1284031659
Supplemental Materials: This information will be provided by the instructor on the first day of class.