Broward Community College
Course Outline

STATUS: A

COMMON COURSE NUMBER: CTS 1311C

COURSE TITLE: Linux Security

CREDIT HOURS: 3

CONTACT HOURS BREAKDOWN:

Lecture/Discussion	40
Lab	8
Other	
Contact Hours/Week	3

CATALOG COURSE DESCRIPTION:

This course covers the fundamentals of security. It examines common security problems, and provides a detailed walk-through of several security-related tools. The course also discusses the proper use of administrative privileges and privacy. The skills developed by students completing this course (in combination with CEN1881C, CEN1882C, and CEN1883C) will help prepare them for the LPI Level 1 certification exams.

Prerequisite: CTS1301C

Corequisite:

UNIT TITLES:

1. Security Vulnerabilities
2. Security Techniques
3. Security Monitoring and System Logs
4. U.S. Law and System Administration
5. Codes of Ethics

I. Course Overview:

Upon successful completion of this course, the students should be able to describe the security issues facing a Linux system administrator, while implementing and administering a secure Linux system.

II. Units:

Unit 1. Security Vulnerabilities

General Outcome:

1.0 The student should be able discuss Linux security problems and identify why security lapses occur.

Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

1.1 Discuss the security vulnerabilities with users and administrators.

1.2 Discuss the security vulnerabilities with software bugs.

1.3 Identify "open doors" created by insecure software programs.

1.4 Discuss security problems in the /etc/passwd and /etc/shadow files.

1.5 Identify improperly set file permissions.

Unit 2. Security Techniques

General Outcome:

2.0 The student should be able to use various security techniques to prevent security breaches.

Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

2.1 Setup Packet filtering to prevent unwanted traffic on the network.

2.2 Identify unnecessary services and stop them, so they will not be used maliciously.

2.3 Obtain and apply software patches as they are released.

2.4 Perform backups of important data.

2.5 Understand the importance of a good password policy.

2.6 Monitor the network; keep a vigilant watch for intruders.

2.7 Discuss common sense security issues.

Unit 3. Security Monitoring and System Logs

General Outcome:

3.0 The student should be able to understand the structure of system logs and discuss the importance of monitoring a Linux network.

Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

3.1 Run various commands and programs to detect and watch for intruders.

3.2 Develop logging policies.

3.3 Identify the location of the syslog and other log files.

3.4 Start and stop the syslog daemon.

3.5 Review the syslog and other log files.

Unit 4. U.S. Law and System Administration

General Outcome:

4.0 The student should be able to discuss the legal issues that a Linux System Administrator faces.

Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

4.1 Discuss the liability a system administrator has with regards to illegal actions on the part of the users.

4.2 Discuss the legality of exporting data encryption technology to other countries.

4.3 Discuss issues concerning copyrighted material.

4.4 Discuss privacy issues that may arise.

4.5 Understand the concept of software licenses.

4.6 Identify spam; and discuss how to prevent it.

Unit 5. Codes of Ethics

General Outcome:

5.0 The student should be able to discuss the trust relationship between themselves, as system administrators, and the users and managers of the system they administer. The student should also be able to define a general code of ethics for system administrators.

Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

5.1 Discuss how to approach sensitive issues with users and managers.

5.2 Identify boundaries that they cannot cross.

5.3 Understand the trust that is given them as system administrators.

5.4 Discuss how not to abuse their power as system administrators.