Miami Dade College

Course Description

CTS 1111| Linux + | 4.00 credits

This course is designed to help students prepare for the CompTIA Linux+ Certification Exam and to teach the skills needed to administer GNU/Linux-based work-stations and servers. Students learn how to plan, install, maintain, document, and troubleshoot GNU/Linux operating system services. Prerequisite: CGS1060 or computer experience is required.

Course Competencies:

Competency 1: The student will demonstrate how to manage the system startup environment of GNU/Linux by:

1. Determining and configuring hardware settings.
2. Describing the boot sequence.
3. Identifying boot files and parameters.
4. Describing and using various run levels.
5. Booting up and shutting down a system.
6. Identifying system files, terms, and utilities.

Competency 2: The student will demonstrate how to install Linux and manage software packages by:

1. Designing a hard disk layout
2. Identifying and describing the basic features of LVM.
3. Selecting and installing a boot manager.
4. Configuring GRUB2. Legacy and GRUB2.
5. Identifying and managing shared libraries.
6. Installing software using package management tools (Debian, RPM and YUM).
7. Installing updates and patches.
8. Using configuration management tools.

Competency 3: The student will demonstrate how to configure the system using a command line interface by:

1. Identifying, describing, and using shell commands.
2. Configuring a shell environment by modifying environment variables.
3. Accessing previous commands and the command history.
4. Processing text streams using commands and utilities.
5. Moving, copying, renaming, and deleting files and directories.
6. Listing files using wildcards and search commands.
7. Redirecting standard input, output, and error messages.
8. Sending the output of one command to another command.
9. Creating, monitoring, and killing active processes.
10. Managing process execution priorities (PS, TOP, NICE, RENICE).
11. Searching for text files using regular expression utilities.
12. Editing files using a terminal text editor (VI, etc.)

Competency 4: The student will demonstrate the ability to use devices, Linux file systems, and the Filesystem Hierarchy Standard (FHS) by:

1. Creating, modifying, and deleting partitions and file systems.
2. Maintaining, monitoring, and troubleshooting file system integrity.
3. Mounting, unmounting, and managing file systems.
4. Setting up, editing, and verifying disk quotas.
5. Managing file and directory access using group permissions.
6. Creating and changing hard and symbolic links.

7. Using links to support administrative tasks.
8. Identifying the correct locations of files and directories under the FHS.

Competency 5: The student will demonstrate how to work with shells, scripting and data management, and desktop environments by:

1. Customizing and using the shell environment.
2. Writing BASH functions from frequently used sequences of commands.
3. Writing and customizing simple shell scripts.
4. Using basic SQL commands to perform data manipulation.
5. Installing and configuring X11, the core component of the Linux GUI.
6. Setting up a display manager.
7. Identifying and configuring basic accessibility and assistive technology settings.

Competency 6: The student will demonstrate how to perform administrative tasks and maintain essential system services by:

1. Configuring client-side domain name resolution (DNS).
2. Describing and configuring the Network Time Protocol (NTP).
3. Describing and configuring the syslog.
4. Describing and configuring a Mail Transfer Agent (MTA).
5. Identifying and describing commonly available MTA programs (postfix, send mail).
6. Configuring and managing printers and printing (CUPS).
7. Identifying privileged and non-privileged states.
8. Defining virtualization/hypervisors concepts.

Competency 7: The student will demonstrate how to secure Linux systems by:

1. Performing security administration tasks.
2. Setting and changing user passwords and password settings.
3. Discovering open ports on a system (Nmap and Netstat).
4. Configuring host (Workstation/Server) security.
5. Describing shadow passwords and how they work.
6. Disabling unnecessary network services.
7. Describing the purpose of TCP wrappers.
8. Securing data using encryption (OpenSSH, GPG, etc.).
9. Configuring auditing capabilities and reviewing event logs.
10. Developing Security Policies, including authentication policies.
11. Performing backups and restoring the system from a backup.
12. Using a host intrusion detection tool.

Competency 8: The student will demonstrate workplace-readiness skills by:

1. Following oral and written instructions.
2. Participating in group discussions as a member and as a leader.
3. Demonstrating self-motivation and responsibility to complete an assigned task.
4. Choosing appropriate actions in situations requiring effective time management.
5. Applying principles and techniques for being a productive member of a team.
6. Identifying and discussing intellectual property rights and licensing issues.
7. Identifying and discussing issues contained within professional codes of conduct.
8. Preparing, outlining, and delivering a short oral presentation.
9. Preparing visual material to support an oral presentation.
10. Using appropriate communication skills, courtesy, and dress in the workplace.

Learning Outcomes:

1. Numbers / Data

2. Information Literacy
3. Ethical Issues
4. Computer / Technology Usage