Introduction to Linux

UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course Dates: June 17-28, 2024

Duration: 2 weeks

Estimated Time Commitment: 10-15 hours per week

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online

Target Audience: IT, OT, or Cybersecurity practitioners

Required Prerequisites / Background: This course requires no prior knowledge of the Linux Operating System. However, working knowledge of computer systems is needed to fully comprehend the materials in this course.

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

Instructor	Email
Dr. Guillermo Francia III	gfranciaiii@uwf.edu
Mr. Amador (JR) Avila	aavila@uwf.edu

Course Description

This course focuses on the fundamentals of the Linux Operating System. The course lectures are supplemented with hands-on exercises to reinforce the learning process. The lectures build upon the National Institute of Standards and Technology (NIST) guidelines documented in the following Special Publications (SP): 800-181 rev 1 (NICE Cybersecurity Workforce Framework), NIST-SP-800-154 (Data-Centric System Threat Modeling), and NIST-SP-800-150 (Guide to Cyber Threat Information Sharing).

The course is divided into 5 modules. Each module includes a discussion segment, assessment, or hands-on exercises as appropriate. Each student is expected to participate actively in the course.

This course introduces the basic concepts of command line interfaces, editing tools, shell scripts, basic system and user account administration, and essential networking to enable a practitioner to take full control of a computer running on a Linux operating system.

This course utilizes a combination of lecture, discussion, and hands-on exercises using a virtual Linux machine through a synchronous (live online instruction) modality via Zoom. No prerequisite required other than a working knowledge of computer systems.

NIST NICE Cybersecurity Workforce Framework Mapping

The course addresses cybersecurity work roles as identified in NIST's Special Publication 800-181 rev 1, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

Cybersecurity Work Roles and Categories:

- System Security Analyst (Operate and Maintain, OM-ANA-001)
- System Administrator (Operate and Maintain, OM-ADM-001)

Learning Outcomes mapped to the NICE Cybersecurity Workforce Framework Tasks:

Upon completion of the course, students will be able to:

- Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data). (T0403)
- Install, update, and troubleshoot systems/servers. (T0418)
- Comply with organization systems administration standard operating procedures. (T0458)
- Administer accounts, network rights, and access to systems and equipment. (T0494)

Knowledge and Skills required to fulfill the above tasks mapped to the NICE Cybersecurity Workforce Framework:

- Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g. process management, directory structure, installed applications) (K0608)
- Knowledge of concepts for operating systems (e.g. Linux, Unix) (K0397)
- Knowledge of forensic implications of operating system structure and operations. (K0433)
- Knowledge of operating system command-line tools. (K0318)
- Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep). (K0129)
- Knowledge of scripting. (K0529)
- Skill in manipulating operating system components (S0067)
- Skill in administering operating systems (S0158)

Course Information

Materials:

No Required Texts

Technical Specifications:

Participants need access to a computer with stable internet connection. They will be required to access the course Leaning Management System (LMS) portal, Canvas. Participants will be logging in to the Florida Cyber Range (FCR) to do all hands-on activities (logins and instructions will be provided before session starts). The course will require internet connection for logging in to FCR.

Each module will have a discussion board that participants will use to post questions and comments related to that module. Instructors will look at the questions and comments and respond as needed.

By enrolling in this course, you agree to abide by the Computing Resources Usage Agreement provided to you.

Grading:

Participants will be assigned a pass/fail grade. Participants must earn a total of 70% or higher on graded assessments to earn a passing grade.

Assessment	**Percentage**
Discussions/Test for Understanding	40%
Projects/Exercises	60%
Total:	**100%**

Course Overview / Schedule

Modules and Lessons	**Assessment**
Module 1: Introduction to Linux Topics: ▪ Background ▪ Flavors of Linux ▪ File System ▪ Basic commands	▪ Quiz ▪ Discussion

Module 1 Hands-on Activity. Topics: ▪ File creation, modification, and deletion	▪ Completion of activity
Module 2: Shell Scripting Topics: ▪ Text editing ▪ Basic shell scripting ▪ Advanced shell scripting	▪ Quiz ▪ Discussion
Module 2 Hands-on activity. Topics: ▪ Shell scripting for system automation	▪ Completion of activity
Module 3: Basic Linux System Administration Topics: ▪ Managing users ▪ Managing file system ▪ System Utilities ▪ System Maintenance	▪ Quiz ▪ Discussion
Module 3 hands-on activity. ▪ Creating and monitoring users	▪ Completion of activity
Module 4: Advanced Linux System Administration Topics: ▪ System Processes ▪ System Monitoring ▪ Security Logging	▪ Quiz ▪ Discussion
Module 4 hands-on activity. ▪ Security automation	▪ Completion of activity
Module 5: Linux network and internetwork Topics: ▪ Network configuration ▪ Routing ▪ Testing	▪ Discussion ▪ Quiz