CENTER FOR CYBERSECURITY
AT THE UNIVERSITY OF WEST FLORIDA

CompTIA Linux+ (XK0-005) Exam Prep

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

Course Overview

Length of Completion: 40 contact hours

Prerequisites: CompTIA A+, Server+ or Network+ certifications, or 1 year experience on IT systems is strongly recommended.

Recommended Schedule: 9 Weeks

Learning Setting: Hybrid Asynchronous Online / Instructor-led Zoom sessions (weekly on Mondays at 5 PM Central)

Target Audience: IT practitioners (with 1+ years experience).

Level of instruction: Undergraduate

Course Instructors:

Instructor	Email Address
Dr. Guillermo Francia, III	gfranciaiii@uwf.edu
Mr. Amador Avila, Jr.	aavila@uwf.edu

Course Description

The CompTIA Linux+ exam verifies that the candidate possesses the fundamental knowledge and proven skills required to:

- Configure, manage, and troubleshoot Linux systems.
- Operate Linux in both on-premises and cloud-based server environments.
- Implement security best practices.
- Use scripting, containerization, and automation to optimize a Linux system.

NIST NICE Cybersecurity Workforce Framework Mapping

The course addresses cybersecurity competency areas and 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 Competency Areas:

- Access Control
- Communications Security
- DevSecOps
- Operating Systems Security

Cybersecurity Work Roles and Categories:

Operate and Maintain

- Technical Support (IO-WRL-007)
- Network Management (IO-WRL-004)
- System Administrator (IO-WRL-005)

Learning Outcomes mapped to the NICE Cybersecurity Workforce Framework Knowledge, Skills and Abilities (KSAs):

Knowledge of computer networking concepts and protocols, and network security methodologies.

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

- T0418: Install, update, and troubleshoot systems/servers
- K0004: Knowledge of cybersecurity and privacy principles.
- T0494: Administer accounts, network rights, and access to systems and equipment.
- K0005: Knowledge of cyber threats and vulnerabilities.
- K0011: Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
- K0029: Knowledge of organization & Local and Wide Area Network connections.
- K0038: Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- K0049: Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- K0088: Knowledge of systems administration concepts.
- K0100: Knowledge of the enterprise information technology (IT) architecture.
- K0104: Knowledge of Virtual Private Network (VPN) security.
- K0158: Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
- K0160: Knowledge of the common attack vectors on the network layer.

- K0167: Knowledge of system administration, network, and operating system hardening techniques.
- K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0292: Knowledge of the operations and processes for incident, problem, and event management.
- K0294: Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.
- S0040: Skill in implementing, maintaining, and improving established network security practices.
- S0076: Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
- S0077: Skill in securing network communications.
- S0079: Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
- S0084: Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
- T0494: Administer accounts, network rights, and access to systems and equipment.

GRADING

The course is designed as examination preparation. Students should complete all assignments and take time to review any incorrect answers. Non-credit course students shall receive a grade of either complete or incomplete at the conclusion of the course. Participants must earn a total of 70% or higher on graded assessments to earn a course completion grade.

Students must register to take the certification exam during the first 10 days of the course and report their exam date(s) to their instructor. Students shall take the certification exam(s) within one week of course end date to receive a course completion certificate and digital badge. Each student will receive a voucher to take the exam and students who do not pass on the first attempt will be provided with additional resources and a second voucher.

Grading Scheme:

Assignment	**Percentage of Grade**
Exam Registration • Register for the CompTIA Linux+ (XK0-005) Exam • Submit Exam Date(s) to the instructor • Due no later than the 6th business day of the course.	15%
CompTIA Certification Exam	10%

• Sit for CompTIA Linux+ (XK0-005) Exam • Submit Candidate Score Reports from the exam to the instructor. • Due no later than five business days after the course ends	
Assignment Completion • Labs • PBQs • Practice Questions	40%
Proficiency	20%
Final CompTIA Practice Assessment	15%
Total	100%

Technical Skills Covered

Exam Blocks	**Weekly Schedule**
Linux Concepts (Lessons 1-4)	1 and 2
Server Administration (Lessons 5-8)	3 and 4
Network Management and Security (Lessons 9-12)	5 and 6
Scripting, Automation, and Installation (Lessons 13-16)	7 and 8

Course Outline

Course Modules

Modules and Lessons	Labs and PBQs
Module 1: (Lessons 1-2) Introduction to Linux and User/Group Administration Topics: ▪ Understand Bash interactions ▪ Use help in Linux ▪ Understand troubleshooting methodology ▪ Manage User Accounts ▪ Manage Group Accounts ▪ Configure Privilege Escalation	1-Assisted Lab: Basic Linux Interaction 2-Assisted Lab: Manage User Accounts 2-Assisted Lab: Manage Group Accounts PBQ Lesson 2: Administering Users and Groups

Module 2: (Lessons 3-4) Configure Permissions and Implement File Management Topics: • Configure Standard Linux Permissions • Configure Access Control Lists (ACL) • Understand the Linux File System • Use File Management Commands • Find File Locations	3-Assisted Lab: Configure Standard Linux Permissions 3-Assisted Lab: Configure Access Control Lists 3-Applied Lab: Identity and Access Control PBQ: Lesson 4: Implementing File Management
Module 3: (Lessons 5-6) Authoring Text Files and Managing Software Topics: ▪ Edit Text Files ▪ Manage Text Files ▪ Understand Software Management ▪ Manage RPM Software Packages and Repositories ▪ Manage Debian-based Software Packages ▪ Compile Source Code ▪ Acquire Software	5-Assisted Lab: Edit Text Files 5-Assisted Lab: Backup, Restore, and Compress Files 6-Assisted Lab: Manage RPM Packages 6-Assisted Lab: Manage DEB Packages PBQ: Lesson 6: Managing Software
Module 4: (Lessons 7-8) Administering Storage and Managing Devices Topics: ▪ Understand Storage ▪ Deploy Storage ▪ Manage Other Storage Options ▪ Troubleshoot Storage ▪ Gather Hardware Information ▪ Manage Processes ▪ Manage Memory ▪ Manage the Linux Kernel	7-Assisted Lab: Deploy Storage and LVM 8-Assisted Lab: Manage Processes PBQ: Managing Devices, Processes, Memory, and the Kernel
Module 5: (Lessons 9-10) Managing Services and Configuring Network Security Topics: ▪ Manage System Services ▪ Configure Common System Services ▪ Configure Localization Settings ▪ Understand Network Fundamentals ▪ Manage Network Settings ▪ Troubleshoot the Network	9- Assisted Lab: Manage Services 10-Assisted Lab: Configure Network Settings 10-Assisted Lab: Configure Remote Administration 10-Applied Lab: System Management PBQ: Lesson 10: Configuring the Network Settings

Module 6: (Lessons 11-12) Configuring Network Security and Managing Linux Security Topics: ▪ Configure Firewall ▪ Monitor Network Traffic ▪ Harden a Linux System ▪ Manage Certificates ▪ Understand Authentication ▪ Configure SELinux	11-Assisted Lab: Configure a Firewall 11-Assisted Lab: Intercept Network Traffic 12-Assisted Lab: Harden a Linux System 12-Assisted Lab: Configure SELinux PBQ: Lesson 11 Configuring Network Security
Module 7: (Lessons 13-14) Implementing Simple Scripts and Using Infrastructure as Code **Topics:** ▪ Understand Bash Scripting Basics ▪ Use Shell Script Elements ▪ Implement Scripts with Logical Controls ▪ Understand Infrastructure as Code ▪ Implement Orchestration ▪ Manage Version Control with Git	13-Assisted Lab: Manage Scripts 14-Assisted Lab: Configure a System with Ansible 14-Assisted Lab: Manage Version Control with Git PBQ: Lesson 13 Implementing Simple Scripts
Module 8: (Lessons 15-16) Managing Containers and Installing Linux **Topics:** ▪ Understand Containers ▪ Deploy Containers ▪ Understand Virtualization Concepts ▪ The Linux Boot Process ▪ Modify Boot Settings ▪ Deploy Linux	15-Assisted Lab: Deploy Containers 16-Assisted Lab: Manage GRUB2 16-Assisted Lab: Deploy a Linux System 16-Applied Lab: Scripting, Configuration Management, and Orchestration PBQ: Lesson 15 Managing Containers in Linux