CA401: Linux Operations

24 Instructional Hours 61 CPEs 37 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER TO INTERMEDIATE

This course provides a comprehensive introduction to Linux system administration and command-line operations with an emphasis on practical, real-world usage. The course covers foundational Linux concepts, including filesystem structure, shell commands, text editors, permissions, and user management, before progressing to advanced topics such as process control, system boot mechanisms, package management, networking, automation with cron, and shell scripting. Students gain hands-on experience configuring, managing, and troubleshooting Linux systems, including secure remote access, network analysis, and system services using systemd. The course also introduces widely used security and networking tools and concludes with a capstone challenge designed to reinforce operational and cybersecurity-relevant skills essential for modern IT and security professionals.

You Will Be Able To

- Navigate and manage Linux systems confidently using essential shell commands and filesystem concepts.
- Create, edit, and manage files safely using common Linux text editors and command-line tools.
- Administer users, groups, and permissions (including ownership and privilege elevation with sudo) to support secure operations.
- Monitor and control system processes, understand the Linux boot process, and manage services with systemd.
- Apply Linux networking fundamentals for troubleshooting, secure remote access (SSH/SCP), and practical system management tasks.

Who Should Attend

This course is designed for a broad audience interested in working with Linux systems and the command-line environment. It is appropriate for students, entry-level professionals, and experienced practitioners who want to develop or reinforce practical skills in system navigation, administration, networking, automation, and troubleshooting. The course supports learners across IT, cybersecurity, software development, cloud, and engineering disciplines, and is structured to be accessible while still providing depth applicable to real-world technical environments.

Relevant Combat Roles

- IT Support
- Systems Administrator (Junior to Mid-Level)
- Linux Administrator
- Cybersecurity Analyst (Entry-Level)
- Network Operations Technician

Topics Covered

Linux command line foundations, filesystem structure, and working efficiently in he terminal (navigation, wildcards, I/O redirection, pipelines).

Administration fundamentals: users/groups, permissions, ownership, archiving/backup, and package management concepts.

Operations and security workflow: processes/signals, boot process + systemd services, networking utilities, SSH/SCP, and task automation with cron and shell scripting.

Labs

User & Group Administration
(configure Linux users/groups, manage permissions and ownership, apply sudo/SUID privileges, and validate access control using chmod/chown/id/su/sudo CLI tools)

Process Monitoring & Service Management
(monitor and control running processes using ps/top/kill/signals, inspect system services with systemctl, and analyze Linux process behavior and resource usage)

Task Automation & Bash Scheduling
(create bash automation workflows, schedule recurring jobs with cron/systemd timers, automate backups and log collection, and validate execution through logs and script output)