LFS216 - Linux Security Fundamentals

Modality: On Demand

Duration: 40 Hours

About This Course:

This program is a detailed look at the security issues that can affect nearly every device, particularly with the smooth communication we are seeking from the Internet. Some of the Linux securing features are either integrated into the Linux Kernel or introduced by the numerous Linux Distributions. This class discusses many of those system-securing choices. Specialized Linux systems are used in some situations showing how one can communicate with corporate production servers. It is a detailed class experience that will further increase your knowledge of security problems and preventive steps.

The session begins with a Computer Security outline and touches on how security impacts everyone in the administration, implementation, development, and end-user chain. This program is intended to operate with a wide variety of Linux distributions so that you can apply these principles whatever your distro.

Upon completion of this training, students will be able to evaluate your existing security requirements, assess your current readiness for security and enforce security options as needed. All engaged with any security-related activities will gain additional skills from this program like implementation managers, developers, and technicians.

Audience:

People at any stage who are concerned with any security-related mission. The course emphasizes comprehension and essential parts configuration so that any technical level is appropriate for learning regarding Linux Security with the solutions offered.

Prerequisites:

Students will be able to access files from the Internet, set up VMs, and install a virtual computer and a virtual private network called "host only." Fundamental Linux command line capabilities, covered in (LFS201-System Administration Essentials) are needed. It is highly recommended that you become familiar with Fedora, CentOS, or Red Hat Linux.

Materials: One Year of online access to all contents of courses and laboratories.

This course is:

- 100% self-paced and online
- Loaded with labs planned by our specialist
- Intended to provide you with the required skills and information to identify your security requirements, determine current security preparedness and enforce security options as appropriate

Course Outline:

Chapter 1. Course Introduction
Chapter 2. Security Basics
Chapter 3. Threats and Risk Assessment
Chapter 4. Physical Access
Chapter 5. Logging
Chapter 6. Auditing and Detection
Chapter 7. Application Security
Chapter 8. Kernel Vulnerabilities
Chapter 9. Authentication
Chapter 10. Local System Security
Chapter 11. Network Security
Chapter 12. Network Services Security
Chapter 13. Denial of Service
Chapter 14. Remote Access
Chapter 15. Firewalling and Packet Filtering
Chapter 16. Response and Mitigation