LINUX SECURITY ESSENTIALS Course

Linux Security Essentials is a course that teaches the fundamentals of securing Linux–based computer systems.

Course Overview

Linux Security Essentials courses typically cover a range of topics, including system hardening, network security, cryptography, vulnerability assessment, incident response, and compliance regulations. The course content may also include hands–on practice and real–world examples to reinforce the concepts learned in the course.

Course outline

1. Introduction to Linux security: This might cover basic security concepts such as CIA triad, security threats and vulnerabilities, and security controls.
2. Securing the Linux operating system: This might cover system hardening, patch management, user and group management, file permissions, and auditing.
3. Network security: This might cover firewall configuration, intrusion detection and prevention, network monitoring, and virtual private networks (VPNs).
4. Cryptography: This might cover encryption algorithms, public key infrastructure (PKI), secure sockets layer/transport layer security (SSL/TLS), and secure shell (SSH) protocols.
5. Application security: This might cover web application security, secure coding practices, database security, and application hardening.
6. Incident response: This might cover incident response planning, threat intelligence, and forensics.
7. Compliance and regulations: This might cover regulatory compliance standards such as PCI DSS, HIPAA, and GDPR, and how to achieve compliance in a Linux environment.

info@gandotech.com
Lisbon, Sintra, Mirante St, No3, 2/C
+351 911970800
P.Code: 27 45-039